# ВСТУП

У 2015 році Міжнародним союзом електрозв'язку (МСЕ) було започатковано перший у своєму роді глобальний план розвитку мереж п'ятого покоління (5G), що актуалізувало необхідність розробки надійних механізмів та процедур безпеки для інфраструктури 5G.

Перспективна технологія обіцяла досягнення значних показників: швидкість передачі даних понад 1 Гбіт/с, затримку менше 1 мс та здатність підтримувати одночасне підключення до 1 мільйона пристроїв на квадратний кілометр. Такі високі вимоги до продуктивності значно вплинули на архітектурні принципи побудови цих мереж.

Ключовою особливістю стала децентралізація, яка передбачає розміщення численних локальних центрів обробки даних на периферії мережі. Це дозволяє мінімізувати затримки при Machine-to-Machine (M2M) комунікації та розвантажити основне мережеве ядро за рахунок обслуговування значної кількості пристроїв Інтернету Речей (IoT). Як наслідок, межі нових поколінь мереж розширюються до рівня базових станцій, що дає змогу створювати локальні комунікаційні центри та надавати хмарні сервіси без ризику критичних затримок або відмов у обслуговуванні.

На відміну від сучасних тенденцій, побудова телекомунікаційних мереж 3G та 4G поколінь традиційно базувалася на роботі з одним або обмеженим колом постачальників (вендорів), які надавали комплексні рішення «апаратне забезпечення – програмне забезпечення». Такий підхід, по суті, передбачав роботу «з-під-коробки»: достатньо було встановити та налаштувати обладнання обраного вендора без необхідності заміни або доповнення пропрієтарного програмного забезпечення. Сучасна галузева практика розвивається в протилежному напрямку, зосереджуючись на віртуалізації мереж, мультивендорній архітектурі та різноманітності програмних рішень. Такі технології, як програмно-визначені мережі (Software-Defined Networking, SDN) та віртуалізація мережевих функцій (Network Functions Virtualization, NFV), набувають все більшої популярності, що

призводить до інтеграції значного обсягу програмного забезпечення з відкритим кодом у процеси та функції управління телекомунікаційними мережами.

Периферійні пристрої, що виконують роль локальних мережевих ядер, відповідають за маршрутизацію користувацького трафіку, обробку запитів, а також локальне кешування та зберігання даних. У такий спосіб зона відповідальності мереж 5G поширюється не лише на центральне ядро, але й на периферійні компоненти, включаючи локальні бази даних та радіоінтерфейси 5G New Radio (5G-NR). Це створює нові вектори атак на обчислювальні ресурси локальних пристроїв, які априорі мають менший рівень захисту порівняно з централізованими вузлами, з метою організації відмови в обслуговуванні. Подібні інциденти можуть призвести до перебоїв у доступі до Інтернету цілих районів, некоректній роботі IoT-пристроїв (наприклад, у рамках системи «розумний дім»), а також до неможливості функціонування сервісу екстрених сповіщень IMS.

До 2025 року архітектура 5G еволюціонувала у напрямку гібридної моделі, що поєднує централізоване ядро з розподіленою мережевою периферією. Ключовою особливістю став перехід до Standalone (SA) архітектури, що дозволило повноцінно реалізувати переваги 5G, включаючи мережеву нарізку (network slicing) та ультра-надійний зв'язок з малою затримкою (URLLC). Активно впроваджується концепція Open RAN, що сприяє розвитку мультивендорних рішень та гнучкості мережевих інфраструктур.

Станом на 2025 рік охоплення 5G у міських агломераціях досягло 85%, тоді як у сільській місцевості триває розгортання мереж з використанням технології Fixed Wireless Access (FWA). Понад 60% операторів впровадили віртуалізацію мережевих функцій (NFV) та програмно-визначені мережі (SDN) для керування ресурсами. Основним трендом стало масове підключення промислових IoT-пристроїв та розвиток приватних мереж 5G для корпоративного сектору, що стимулювало появу спеціалізованих мережевих нарізок для різних галузей промисловості.

Актуальність теми обумовлена інтенсивним переходом телекомунікаційних операторів на архітектури 5G та необхідністю ефективного управління складними

гетерогенними мережами. Впровадження технологій мережевої віртуалізації (NFV) у поєднанні з програмно-визначеними мережами (SDN) стало ключовим фактором забезпечення гнучкості, масштабованості та економічної ефективності інфраструктури. Однак відсутність уніфікованої методики оцінки ефективності цих рішень призводить до неефективного використання ресурсів, ускладнює порівняння технологічних платформ і гальмує оптимізацію мережевих архітектур. Розробка комплексної методики дозволить об’єктивно оцінювати продуктивність, ресурсну ефективність та операційні витрати різних віртуалізаційних рішень, що є критично важливим для прискорення розгортання 5G-мереж, забезпечення якості послуг і підвищення конкурентоспроможності операторів зв’язку.

Мета роботи:

Об’єкт роботи:

Предмет роботи:

Завдання, які будуть виконуватись:

# 1 АНАЛІТИЧНИЙ ОГЛЯД ТЕХНОЛОГІЙ ТА ПЛАТФОРМ ДЛЯ ПОБУДОВИ 5G МЕРЕЖ НА ОСНОВІ SDN ТА NFV

## 1.1 Вимоги телекомунікаційних систем п'ятого покоління (5G) до інфраструктури та управління мережею

Є необхідність в проведенні системного дослідження архітектурних рішень, віртуалізаційних платформ і програмно-визначених інструментів управління, що формують основу сучасних телекомунікаційних систем п'ятого покоління. У рамках такого огляду аналізуються провідні стандартизовані архітектури, платформи віртуалізації мережевих функцій (NFVI), рішення для оркестрації, а також SDN-контролери з підтримкою протоколів OpenFlow. Критичному порівнянню підлягають показники продуктивності, масштабованості, інтеграційної сумісності та операційної ефективності різних технологічних стеків, що дозволяє визначити оптимальні комбінації програмних та апаратних рішень для реалізації конкретних сценаріїв використання 5G, таких як мережева нарізка, обчислення на периферії та обслуговування масивного IoT.

Сучасні мережі 5G пред'являють безпрецедентні вимоги до продуктивності інфраструктури, зокрема забезпечення пікової швидкості передачі даних до 20 Гбіт/с та ультра-низької затримки на рівні 1 мс. Ці показники є критично важливими для підтримки таких інноваційних сервісів, як віртуальна та доповнена реальність, телемедицина та автономні транспортні системи, де стабільність з'єднання відіграє вирішальну роль.

Ключовою вимогою до архітектури є підтримка масивного підключення IoT-пристроїв з щільністю до 1 мільйона пристроїв на км². Це вимагає реалізації ефективних механізмів управління ресурсами, адаптивної маршрутизації та оптимізованого використання радіочастотного спектру для уникнення перевантаження мережі.

Архітектура мережі повинна забезпечувати високу гнучкість через впровадження технологій віртуалізації (NFV) та програмно-визначених мереж

(SDN). Це дозволяє динамічно створювати віртуальні мережеві сегменти (network slicing) з індивідуальними параметрами для різних категорій клієнтів та сервісів.

Надійність та енергоефективність становлять основу вимог до інфраструктури, зокрема забезпечення 99.999% доступності сервісів для критично важливих застосунків. Одночасно необхідно мінімізувати енергоспоживання обладнання через використання адаптивних алгоритмів керування потужністю та оптимізації роботи мережевих компонентів.

Управління мережею має ґрунтуватися на принципах автономності та інтелектуального аналізу даних з використанням штучного інтелекту. Це включає прогнозування навантаження, проактивне виявлення аномалій, автоматичне масштабування ресурсів та само відновлювані функції для забезпечення безперервності обслуговування.

Ключові принципи архітектури мереж 5G формують основу для розуміння функціональності програмних модулів та механізмів безпеки. Основними архітектурними принципами є:

Принцип розділення площин передбачає декомпозицію мережевих вузлів на елементи користувацької площини (User Plane) та площини управління (Control Plane), що забезпечує гнучкість масштабування та розгортання мережі з можливістю централізованого чи децентралізованого розміщення компонентів.

Сервісно-орієнтована архітектура реалізується через механізм мережевих нарізок (network slicing), що дозволяє створювати віртуальні мережі, адаптовані під конкретні сервіси та групи користувачів.

Віртуалізація мережевих функцій є обов'язковою умовою, де всі мережеві елементи реалізуються як віртуальні функції (VNF).

Конвергентна архітектура забезпечує об'єднання різних типів мереж доступу (3GPP 5G NR та non-3GPP) з єдиним ядром мережі, підтримуючи єдині алгоритми аутентифікації незалежно від типу доступу.

Розподілені обчислення реалізуються через підтримку одночасного доступу до централізованих та локальних сервісів з використанням концепцій хмарних та периферійних обчислень.

Сучасні підходи до архітектури включають підтримку мережевих функцій без збереження стану (stateless), де обчислювальні ресурси відокремлені від сховищ даних, а також гнучку підтримку роумингу з маршрутизацією трафіку через домашню мережу або з локальним "приземленням" у гостевій мережі.

Міжфункціональна взаємодія реалізується двома способами: сервіс-орієнтованим (service-based) та інтерфейсним (point-to-point), що забезпечує гнучкість комунікації між мережевими функціями. Ці принципи створюють фундамент для побудови масштабованої, гнучкої та ефективної інфраструктури 5G.

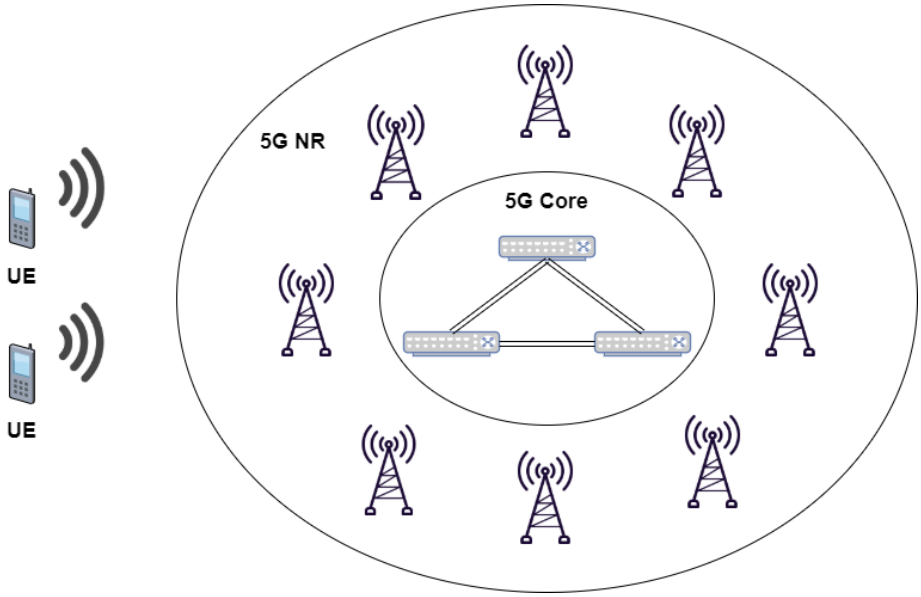



Рис. 1.1 Структура мережі 5G

Основні програмні модулі та мережні функції 5G:

Функція управління доступом та мобільністю (AMF) відповідає за організацію інтерфейсів площини управління, обмін сигнальним трафіком RRC та NAS з наступним шифруванням і захистом цілісності даних. Вона управляє реєстрацією користувацького обладнання в мережі, контролює стани підключення та відповідає за доступність обладнання у стані CM-IDLE. Крім того, AMF здійснює управління мобільністю у стані CM-CONNECTED, забезпечує передачу коротких повідомлень між обладнанням користувача та SMF, керує службами геолокації та виділяє ідентифікатор потоку EPS для взаємодії з системами попереднього покоління.

Функція управління сесіями (SMF) виконує комплексне управління сесіями зв'язку, включаючи створення, модифікацію та закриття сесій з підтримкою тунелю між мережею доступу та UPF. Вона займається розподілом IP-адрес користувацького обладнання, вибором відповідного шлюзу UPF та взаємодією з PCF. Функція включає управління політиками якості обслуговування (QoS), динамічну конфігурацію обладнання за допомогою DHCP-протоколів, контроль збору даних для тарифікації та забезпечення безперервності сервісів (SSC). Додатково SMF організовує взаємодію з гостовими мережами під час роумингу.

Функція користувацької площини (UPF) забезпечує підключення до зовнішніх мереж передачі даних, включаючи глобальний Інтернет, та виконує маршрутизацію пакетів користувачів. Вона відповідає за маркування пакетів відповідно до політик QoS, діагностику трафіку з виявленням додатків на основі сигнатур і надання звітів про використання трафіку. UPF також слугує якірною точкою для підтримки мобільності всередині однієї та між різними технологіями радіодоступу.

Уніфіковане управління даними (UDM) здійснює керування профілями користувачів, зберігаючи та модифікуючи перелік доступних сервісів і відповідних параметрів. Функція включає управління ідентифікаторами SUPI, генерацію облікових даних для аутентифікації 3GPP AKA та авторизацію доступу на основі профілю. UDM також відповідає за управління реєстрацією користувачів, підтримку безперервності обслуговування, управління доставкою SMS і може мати декілька екземплярів для обслуговування одного користувача.

Сховище уніфікованих даних (UDR) виконує функцію централізованого сховища різноманітних користувацьких даних і є, по суті, комплексною базою даних усіх абонентів мережі. Разом з функцією зберігання неструктурованих даних (UDSF), яка зберігає контексти зареєстрованих користувачів, UDR забезпечує безперервність сервісів при плановому чи аварійному виведенні AMF з експлуатації. Типовою практикою є розміщення UDR та UDSF на одній фізичній платформі.

Функція контролю політик (PCF) формує та призначає користувачам політики обслуговування, включаючи параметри якості обслуговування (QoS) та правила тарифікації. На основі вимог сервісу, завантаженості мережі та обсягу трафіку функція динамічно створює віртуальні канали з різними характеристиками. PCF забезпечує оптимальне розподілення мережних ресурсів відповідно до поточних потреб.

Функція мережевої експозиції (NEF) організовує безпечну взаємодію зовнішніх платформ і додатків з ядром мережі, надаючи контроль над параметрами QoS та правилами тарифікації для окремих користувачів. Ця функція слугує безпечним шлюзом для інтеграції сторонніх сервісів з інфраструктурою 5G.

Система функцій безпеки включає: SEAF, яка разом з AUSF забезпечує аутентифікацію користувачів; AUSF, що діє як сервер аутентифікації; ARPF, яка зберігає криптографічні ключі та генерує вектори аутентифікації; SCMF для управління контекстом безпеки; SPCF для застосування політик безпеки з урахуванням можливостей мережі та обладнання; та SIDF, яка виконує дешифрування ідентифікатора користувача (SUPI) з прихованого ідентифікатора (SUCI).

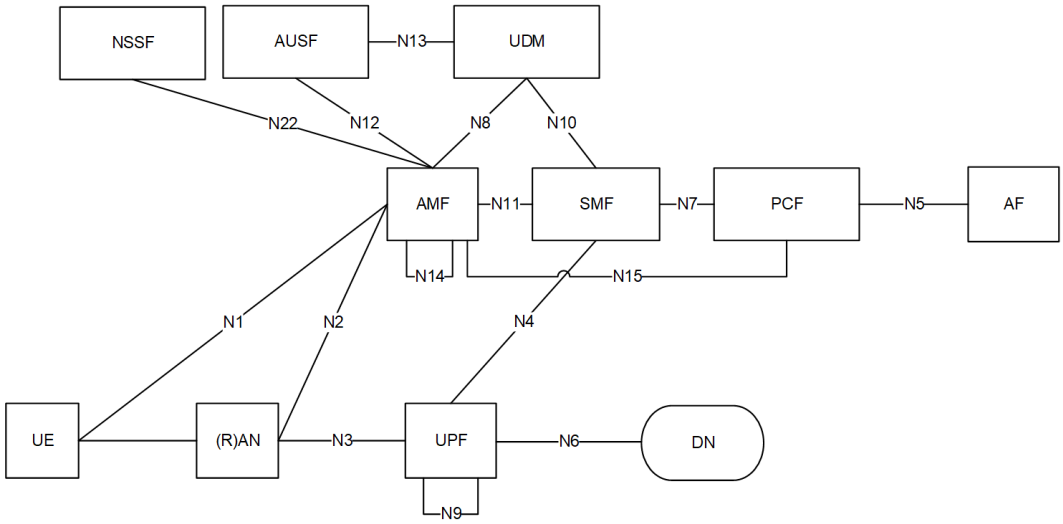



Рис. 1.2 Функціональна архітектура ядра мережі 5G

Гнучкість мережі забезпечується за рахунок мережевих зрізів (network slicing), які поділяють одну фізичну мережу на кілька шарів, кожен з яких має власні

налаштування, адаптовані під конкретну послугу. Таким чином, знижуються витрати, забезпечується ефективність та гнучкість майбутніх сервісів.

Сегментування здійснюється завдяки використанню технологій NFV (віртуалізації мережевих функцій) та SDN (програмно-визначених мереж). Для того щоб конкретний окремий сегмент мережі забезпечував ефективну роботу певного набору послуг, він має бути прив'язаний до різних елементів інфраструктури, включаючи VPN, хмарні сервіси та технології доступу, а також через VNF (віртуалізовані мережеві функції) – до ресурсів транспортної мережі.

Мережеве сегментування знижує бізнес-ризики, пов'язані з запуском нових послуг, оскільки проблеми в одному сегменті не впливають на функціонування послуг, за які відповідає інший сегмент. Крім того, використання сегментування забезпечує безпроблемну міграцію.

Мережева архітектура має змінюватися з появою нових стандартів зв'язку, і відмова від підходу, за якого всі послуги надаються на єдиній мережі, на користь мережевого сегментування спрощує це завдання. Використання таких механізмів, як Dedicated Core Network (DCN) – це один із кроків у правильному напрямку.

Для забезпечення гнучкості мережі 5G необхідно впроваджувати різноманітне апаратне забезпечення, на базі якого у різних фізичних сегментах мережі розгортатиметься відповідний функціонал. Особливу увагу слід приділити проектуванню рівня користувацьких даних (user plane), який має забезпечувати високу пропускну здатність. Наприклад, можливий сценарій, коли більша частина трафіку вимагає лише простий обробки, і для цього достатньо спрощеного апаратного забезпечення. Водночас інша частина трафіку може потребувати складнішої обробки. Економічно ефективне масштабування рівня користувацьких даних, розраховане під одну смугу частот або декілька агрегованих смуг, є ключовим компонентом транспортної мережі 5G.

Можливість розділення функцій рівня управління (control plane) та рівня користувацьких даних (user plane) відіграє одну з ключових ролей в архітектурі транспортної мережі п'ятого покоління. Таке розділення дозволяє масштабувати ресурси рівнів управління та даних незалежно один від одного. Воно також дає

змогу розміщувати ресурси цих рівнів на різних ділянках мережі. Наприклад, рівень управління можна розташувати на центральному майданчику, спростивши таким чином процеси керування та експлуатації. Рівень користувацьких даних може бути розподілений по декількох локальних майданчиках, щоб знаходитися якомога ближче до користувачів. У результаті скорочується час проходження сигналу, і для передачі даних за одиницю часу потрібна менша ширина смуги пропускання. Цей підхід добре підходить, зокрема, для кешування контенту, оскільки в цьому випадку потрібна менша пропускна здатність для передачі певного обсягу даних між базовими станціями.

Оскільки розділення рівня управління та рівня користувацьких даних є основою концепції SDN, використання програмно-конфігурованих мереж значно підвищує гнучкість транспортної мережі 5G. Функціонал рівня управління зазвичай включає керування даними про місцезнаходження, узгодження політик та аутентифікацію сесій. Таким чином, розділення на цьому рівні є абсолютно природним.

Функціонал рівня користувацьких даних може розгортатися відповідно до конкретних сценаріїв використання. Оскільки потреби в підключенні відрізняються для різних сценаріїв, створення унікальних конфігурацій для кожного з них буде найбільш економічно ефективним. Наприклад, M2M-підключення мають невеликий обсяг корисної навантаження та обмежену мобільність, тоді як сервіси eMBB (enhanced Mobile Broadband) характеризуються великими обсягами даних та високою мобільністю. Сервіси eMBB можна розбивати на декілька простіших послуг, таких як потокове відео та веб-серфінг, що дасть змогу розгортати їх як окремі сегменти в межах одного шару. Такий підхід у підсумку допомагає підвищити гнучкість транспортної мережі.

Очевидно, що для розвитку бізнесу необхідно будувати мережу з високим рівнем гнучкості, і саме мережеве сегментування дозволяє досягти цієї мети. Однак підвищення гнучкості може призвести до ускладнення всіх рівнів системи, а отже – до подорожчання операцій та збільшення часу їх виконання. Вирішенням цієї проблеми є автоматизація.

Управління мережею має враховувати три основні етапи життєвого циклу послуги: створення, активація та експлуатація:

- Створення нових послуг або кастомізація існуючих з мінімальним часом виведення на ринок — дозволяє за потреби розбити рішення на компоненти та швидко створювати, виконувати та перевіряти послуги та сегменти;

- Активація послуги з мінімальним показником Time-to-Service (TTS) — дозволяє автоматично активувати сервіс у найкоротші терміни;

- Час виконання (експлуатація) – надання користувачеві затребуваних можливостей, моніторинг роботи послуги та SLA, адаптація до мінливих умов, забезпечення масштабування нових послуг, кожен з цих процесів має бути повністю автоматизований.

Переваги мережевого сегментування, при якому кожен сегмент має власні характеристики, підтримуються двома рівнями функціоналу управління. Один рівень відповідає за послуги та продукти, серед яких B2B-рішення. Інший рівень відповідає за власне мережеве сегментування. Це наочно показано на наступному рисунку. Інноваційні пропозиції можна створювати шляхом об'єднання функціоналу різних шарів, де один сегмент може мати низьку пропускну здатність і велику затримку, а інший – високу пропускну здатність і малу затримку. Кожна інноваційна пропозиція включатиме такий набір характеристик, як SLA, бізнес-політики та функції контролю всередині сегмента.

## 1.2 Архітектура та принципи роботи програмно-визначених мереж (SDN)

Сучасний корпоративний телеком-ринок перебуває під впливом низки трансформаційних трендів: масове зростання IoT-пристроїв, експоненційне збільшення обсягів даних, активний розвиток хмарних сервісів, політики BYOD (Bring Your Own Device) та технологій Big Data. Це спричиняє стрімке зростання мережевого трафіку та формує потребу бізнесу в гнучкому масштабуванні мережевих інфраструктур. Історично склалося, що мережева інфраструктура відставала в темпах віртуалізації від серверних компонентів і систем зберігання

даних, що робило її "вузьким місцем" сучасної IT-архітектури. Вирішення цієї проблеми став можливим завдяки появі технології програмно-конфігурованих мереж (SDN).

Програмно-конфігуровані мережі (SDN) — це архітектура передачі даних, що передбачає відокремлення рівня управління від рівня передачі даних та його програмну реалізацію. Ключовою проблемою традиційних мереж є їх статичність, що суперечить динамічним вимогам сучасних обчислювальних процесів. Сьогоднішні додатки розподілені між численними віртуальними машинами, що активно взаємодіють між собою, що призводить до домінування "схід-західного" трафіку над традиційним "північ-південь". Часта міграція віртуальних машин для оптимізації навантаження робить традиційні схеми адресації та управління трафіком неефективними.

Архітектура SDN ґрунтується на принципі відокремлення функцій передачі трафіку від функцій управління. На відміну від традиційних рішень, де ці процеси інтегровані в одному обладнанні, SDN передбачає централізоване управління через програмний контролер. Основним протоколом взаємодії в архітектурі SDN виступає OpenFlow, який дозволяє контролеру керувати таблицями потоків комутаторів для формування оптимальних мережевих з'єднань із заданими параметрами.

Сфери застосування SDN включають:

- Побудову хмарних інфраструктур із автоматизованим виділенням мережевих ресурсів;
- Оптимізацію великих центрів обробки даних через централізацію управління;
- Реалізацію концепції "Інтернету речей" (IoT);
- Забезпечення динамічного управління мережевими потоками.

Ця технологія дозволяє ефективно керувати мережевими ресурсами, забезпечуючи гнучкість та масштабованість, необхідні сучасним бізнес-додаткам.

Архітектура програмно-конфігурованих мереж (SDN) базується на трьох ключових рівнях:

Інфраструктурний рівень складається з фізичних або віртуальних мережевих пристроїв (комутаторів та каналів передачі даних), які використовують універсальні таблиці потоків. Ці таблиці формуються та керуються зовнішнім контролером через протокол OpenFlow, що є основним стандартом взаємодії в архітектурі SDN.




Рис. 1.3 Приклад таблиці потоків комутатора.

Рівень управління представлений мережевою операційною системою, яка виконує функцію централізованого контролера. Він забезпечує:

- Програмні інтерфейси (API) для взаємодії з прикладними рішеннями;
- Уніфіковане керування різнорідним мережевим обладнанням;
- Абстрагування мережевої інфраструктури у вигляді єдиного логічного комутатора.

Прикладний рівень містить спеціалізовані програми для високорівневого управління, що реалізують:

- Функції безпеки (мережеві екрани, системи виявлення вторгнень);
- Балансування навантаження;
- Інжиніринг трафіку;

- Керування мобільністю та енергоефективністю.

Ключові переваги SDN включають:

- Вендоронезалежний контроль мережевої інфраструктури;
- Централізоване управління з єдиної точки;
- Спрощення конфігурування та адміністрування;
- Можливість динамічної адаптації мережі до змінних умов;
- Скорочення часу впровадження нових сервісів.

Таким чином, SDN представляє собою трансформаційний підхід до побудови мережевих інфраструктур, що забезпечує гнучкість, автоматизацію та ефективність управління сучасними телекомунікаційними системами.

OpenFlow відокремлює один від одного функції тракту даних і тракту управління, що традиційно реалізуються комутаторами, представлено на рисунку 1.4.

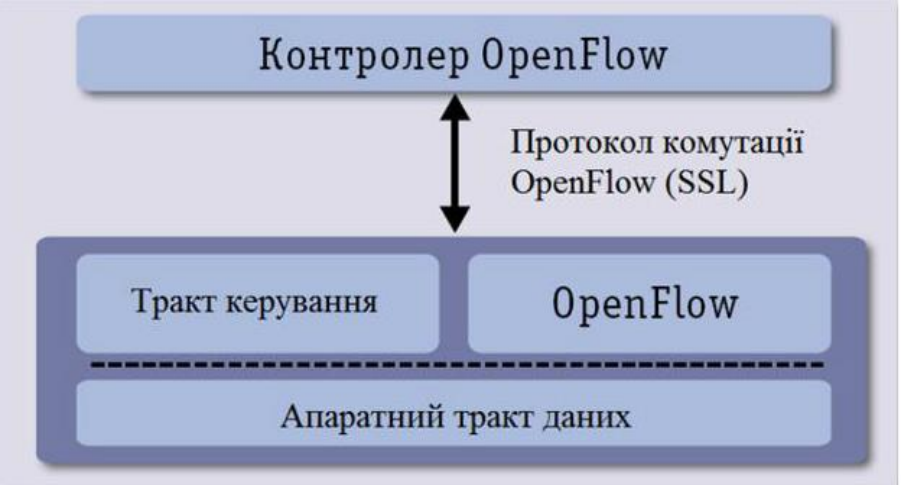



Рис. 1.4 Схематичне зображення принципу роботи протоколу OpenFlow

Архітектура програмно-конфігурованих мереж (SDN) ґрунтується на фундаментальному принципі розділення площини управління (Control Plane) та площини передачі даних (Data Plane). На відміну від традиційних мереж, де обидві функції інтегровані в кожному пристрої, SDN передбачає централізоване управління через спеціалізований контролер, який містить повну інформацію про топологію та конфігурацію мережі.

Ключовим елементом SDN є протокол OpenFlow, розроблений у Стенфордському університеті та стандартизований консорціумом Open Networking Forum. Цей протокол використовує концепцію потоків (flows) і таблиць потоків (Flow Tables) у комутаторах. Таблиця потоків містить:

- Поля відповідності (MAC-адреси, IP-адреси, VLAN ID, порти TCP/UDP);
- Пріоритети обробки потоків;
- Дії, що застосовуються до пакетів (пересилання, модифікація, скидання).

Принцип роботи OpenFlow полягає в тому, що контролер динамічно керує таблицями потоків, додаючи, змінюючи та видаляючи записи. Комутатори виконують лише базові функції передачі даних, а всі складні рішення щодо маршрутизації приймаються централізовано.

Переваги впровадження SDN та OpenFlow включають:

- Використання недорогого обладнання з мінімальною інтелектуальною складовою;
- Централізоване управління гетерогенними мережевими інфраструктурами;
- Можливість швидкої реконфігурації мережі без фізичних змін;
- Створення віртуальних мережевих топологій для різних сервісів;
- Спрощення додавання нової функціональності через єдині API;

Для хмарних середовищ та центрів обробки даних SDN забезпечує необхідний рівень автоматизації та гнучкості, дозволяючи оперативно виділяти мережеві ресурси та оркеструвати роботу великих груп комутаторів. Це особливо важливо для забезпечення мобільності віртуальних машин, балансування навантаження та ефективного управління трафіком.

### 1.3 Надійність в мережах з використанням принципів побудови SDN

Згідно загального опису, надійність – це властивість об’єкту зберігати у визначених межах значення всіх параметрів, які характеризують здатність виконувати необхідні функції в заданих режимах і умовах використання, технічного обслуговування, зберігання і транспортування.

Надійність є одним із ключових показників надійності телекомунікаційної мережі.

Новий напрям аналізу надійності мережі, орієнтований на ідентифікацію каналів передачі та ключових параметрів ефективності безпроводових телекомунікаційних мереж. Провайдери, постачальники послуг і оператори мереж зв'язку прагнуть підвищити надійність роботи телекомунікаційної мережі, тобто здатність мережі виконувати функції передачі з надійністю, яка установлена нормами, протягом тривалого часу. Таким чином, розробка методів її підвищення є актуальною задачею на сьогоднішній день.

Для досягнення необхідної надійності може бути використано різноманітні методи та засоби. У кожної системи свій рівень доступної надійності, так як наслідки відмов різних систем можуть значно відрізнятися. Надійність елементів задається часом на відмову або ймовірністю відмови за визначений проміжок часу. Якщо надійність мережі визначити як надійність усіх елементів, то вона буде рівна нулю.

Для мереж зв'язку, які є складними багатофункціональними системами із великою кількістю різних за своїми властивостям пристроїв (за показниками надійності, за призначенням, термінами введення в експлуатацію, за умовам функціонування), можна виділити два аспекти надійності: апаратурний і структурний.

Під апаратурним аспектом розуміється проблема забезпечення надійності апаратури, окремих пристроїв і їх елементів, які утворюють мережу зв'язку. Розглянувши структуру мережі видно, що вона складається з каналів зв'язку, робочих станцій, серверів, перемикачів, маршрутизаторів. У випадку коли робоча станція вийде з ладу, то це відчує лише користувач, але інші користувачі цього навіть не помітять. Коли з ладу вийде сервер, то це відчують усі клієнти даного серверу, у тому числі і віддалені. Вихід з ладу маршрутизатора може вплинути на роботу цілого регіону. Звідси видно, що окремі вузли можуть по різному впливати на роботу мережі в цілому.

Можна виділити групи різного впливу серед серверів. Наприклад, відмова серверу INADDR.ARPA (доменний сервер, який призначений для визначення імені вузлу по його IPv4- адресі) практичного паралізує роботу програм traceroute (укр. «трейсроут», службова комп'ютерна програма, яка призначена для визначення маршруту слідування даних в мережах TCP/IP). Ще гіршу дію викликає вихід з ладу регіонального серверу DNS(англ. Domain Name System– система доменних імен – комп'ютерна розподілена система для отримання інформації про домени). Саме тому такі сервери зазвичай дублюються. Існують і інші сервери, які впливають на реалізацію певних мережних функцій (поштові сервери, сервери баз даних, сервери центрів сертифікацій та інше). Звідси видно, що вплив на надійність мережі може виконувати не тільки обладнання або операційна система, але і прикладні програми.

Структурний аспект надійності відображає функціонування мережі в цілому в залежності від стану вузлів і ліній зв'язку. Структурна надійність мережі пов'язана з можливістю існування шляхів доставки інформації між кореспондуючими вузлами або пунктами зв'язку мережі.

У випадку, коли користувач не може отримати доступ до певного мережевого ресурсу, це досить часто пов'язано не з відмовою обладнання чи програми, а просто з перезавантаженням однієї з ділянок мережі на шляху до зазначеного ресурсу. Це може виникнути внаслідок недостатньої пропускної здатності і призвести до можливого збільшення затримки доставки, що досить критично у випадку, наприклад, IP-телефонії або відеоконференції. Таким чином, параметри надійності часто залежать від вектору загрузок.

По цій причині, формулюючи задачу оцінки надійності, необхідно визначити які з параметрів важливі: зв'язність, пропускна здатність, час відновлення зв'язності чи мінімізація затримок.

Розглянемо можливість поліпшення надійності доставки інформації, на прикладі програмно-конфігурованих мереж. SDN – програмно конфігуруванні мережі, задача яких спростити керування та адміністрування мережі передачі даних за рахунок декомпозиції площини керування, хоча і шляхом внесення

ускладнень в архітектуру мережі. Згідно IETF: SDN — підхід до побудови мереж, який забезпечує пряме керування ресурсами і мережами, а також їх розподілом за рахунок власних засобів обробки, адміністрування і програмного керування за допомогою відкритих мережних інтерфейсів і абстракції (абстрагування, ізоляції) рівня мережі.

До мереж SDN також пред'являються високі вимоги до надійності (відмовостійкості), у тому числі до характеристик відновлення мережі після відмови, яка повинна виконуватися не помітно для користувача за час не більший 50 мс. Високий рівень відмовостійкості мережі забезпечується за рахунок швидкого виявлення пошкоджень і усунення наслідків за короткий час.

Такий підхід має ряд істотних переваг. По-перше, істотно спрощується сам процес створення маршрутів. На відміну від сьогоднішньої мережі, де маршрутизація – це розподілений інтерактивний процес, при якому робоча топологія мережі «вираховується» спільно усіма пристроями, в SDN – це програма моделювання мережі із заданими параметрами. Використання цієї мережі відкриває нові можливості для створення мережі з вимогами, немислимими у плані традиційного інжинірингу трафіку (Traffic Engineering, TI -методи і механізми, які дозволяють досягти збалансованого завантаження всіх ресурсів мережі шляхом раціонального вибору шляхів проходження трафіку через мережу) і з використанням стандартних протоколів маршрутизації.

Розглянемо в якості прикладу реконфігурацію мережі у випадку падіння каналу між будь-якими вузлами. В традиційній моделі маршрутизатор, підключений до цього каналу, сповістить своїм сусідам про цю подію і всі вони незалежно почнуть розробляти нові маршрути. При цьому вони будуть розповсюджувати інформацію про зміну топології своїм сусідам. Нарешті цей ітераційний процес закінчиться і мережа перейде до нового стану. В залежності від складності мережі і протоколів маршрутизації, які використовуються на ній, цей процес може зайняти більше або менше часу, але якщо враховувати затримки при передачі інформації, кожна ітерація виникне зовсім не миттєво. Більш того, цей

процес не є детермінованим, іншими словами, якщо виникне повторне падіння того ж каналу – не факт,що мережа перейде у той же стан.

У випадку використання керуючого центру розрахунок нової топології виконується виходячи із знання всієї мережі в цілому. Ми також можемо задати необхідну топологію наступного стану. Нарешті, оскільки створення нової топології – це число розрахункових процесів, воно може бути виконано значно швидше.

По-друге, значно збільшуються можливості інновацій. В традиційній розподіленій моделі необхідно приведення функціональності до загального знаменника для можливості взаємодії між незалежними пристроями визначає значну консервативність системи по відношенню до новизни. В SDN інновація – це питання написання нового додатку.

По-третє, замість складних і дорогих маршрутизаторів можна використовувати більш прості пристрої.

SDN-контролер виконує роль центрального мозкового центру в архітектурі 5G, забезпечуючи динамічне та програмоване управління мережевими потоками. Він функціонує як єдина точка прийняття рішень, яка глобально бачить всю мережеву топологію, стан каналів зв'язку та розподіл ресурсів. Завдяки програмним інтерфейсам (API) контролер отримує актуальну інформацію від мережевих елементів і на підставі заданих політик визначає оптимальні шляхи для передачі трафіку. Це дозволяє реалізувати централізоване управління потоками даних у режимі, близькому до реального часу.

Ключовою функцією контролера є реалізація політик Quality of Service (QoS) для різних типів трафіку 5G. Він динамічно класифікує потоки даних від різних сервісів (наприклад, eMBB, URLLC, mMTC) і призначає їм відповідні пріоритети, гарантуючи дотримання SLA. Контролер безпосередньо конфігурує таблиці потоків у комутаторах та маршрутизаторах через протокол OpenFlow, вказуючи, як обробляти кожен тип трафіку — від резервування пропускної здатності для сервісів з ультра-низькою затримкою до маршрутизації масивного IoT-трафіку найефективнішими шляхами.

Важливим аспектом є інтеграція контролера з оркестратором NFV для створення енд-ту-енд мережевих зрізів (network slicing). Контролер відповідає за динамічне створення, модифікацію та моніторинг виділених віртуальних мереж для різних клієнтів або сервісів. Він автоматично виділяє необхідні мережеві ресурси (пропускну здатність, буфери, порти) для кожного зрізу, забезпечуючи його ізоляцію та прогнозовану продуктивність, що є критичним для мультитенантних мереж 5G.

Контролер забезпечує адаптивне управління мережевими потоками в умовах мінливого навантаження та мобільності користувачів. Він постійно аналізує статистику використання мережі та за допомогою алгоритмів машинного навчання прогнозує піки навантаження. Це дозволяє проактивно перенаправляти потоки даних, перерозподіляти ресурси та запобігати перевантаженням. У разі руху абонента між базовими станціями контролер забезпечує безперервність сервісу шляхом миттєвого оновлення правил маршрутизації.

Оркестрація безпеки мережевих потоків є ще одним критично важливим завданням SDN-контролера. Він може автоматично виявляти аномальну поведінку трафіку, ідентифікувати потенційні DDoS-атаки та блокувати шкідливі потоки шляхом оновлення правил у комутаторах. Інтегрований з системами бізнес-політик, контролер забезпечує відповідність потоків даних корпоративним вимогам безпеки, реалізуючи механізми мікросегментації та застосовуючи політики безпеки для кожного окремого потоку в мережі 5G.

## 1.4. Концепція віртуалізації мережевих функцій (NFV) та її синергія з SDN

Стрімке зростання мережевого трафіку та кількості підключених пристроїв робить управління великомасштабними мережами надзвичайно складним завданням. Особливістю сучасних віртуалізованих середовищ є домінування "схід-західного" трафіку між серверами, на відміну від традиційного "північ-південь" трафіку. Це потребує корінних змін у підходах до побудови мереж, що призвело до

появи технологій SDN (Programno-визначені мережі) та NFV (віртуалізація мережевих функцій).

SDN передбачає фундаментальну зміну архітектури мережі шляхом розділення площини управління та передачі даних, централізації управління та автоматизації адміністрування. NFV зосереджена на віртуалізації мережевих функцій (наприклад, брандмауер, NAT, DPI) та їх перенесенні зі спеціалізованих пристроїв на стандартні сервери. Хоці ці технології різні, вони органічно доповнюють одна одну, спрямовані на програмне керування мережею.

Концепція NFV дозволяє розгортати мережеві рішення як програмні додатки, що працюють на стандартному серверному обладнанні. Це знижує залежність від дорогих спеціалізованих пристроїв та значно скорочує операційні витрати. VNF (віртуалізовані мережеві функції) можуть включати одну або кілька віртуальних машин і розгортатися в ЦОД, мережевих вузлах або на клієнтському обладнанні.

На сьогодні SDN в основному використовують великі компанії та інтернет-гіганти, особливо в хмарних платформах і ЦОД. Технологія NFV знаходить застосування в маршрутизаторах, міжмережевих екранах, шлюзах та інших мережевих пристроях у середовищах операторів зв'язку. Обидві технології дозволяють використовувати стандартне недороге обладнання замість спеціалізованих рішень.

Спільне використання SDN і NFV дозволяє абстрагувати послуги не тільки від обладнання, але й від його фізичного місцезнаходження. Це відкриває можливості для розподілу послуг по всій мережі замість їх локалізації в конкретних вузлах. Такий підхід особливо цінний для оркестрації, автоматизації та створення гнучких хмарних платформ, що відповідають вимогам сучасних телекомунікаційних систем.

SDN передбачає розділення площини управління та площини даних. Для керування трафіком використовують контролери на базі ПЗ або API-інтерфейси.

У випадку NFV пропрієтарні мережеві пристрої (наприклад, комутатори та брандмауери) замінюють програмними версіями, розгорнутими на стандартному обладнанні. Головний компонент — віртуальні мережеві функції (VNF) —

віртуалізовані інстанси маршрутизаторів та інших пристроїв під керуванням гіпервізора.

Думки щодо роботи з SDN та NFV склалися полярні. На користь технологій мережевої віртуалізації говорить той факт, що їх уже використовують оператори центрів обробки даних та корпорації для розгортання високопродуктивних додатків.

Організації зі складними розподіленими мережами передачі задіюють SDN та NFV з метою модернізації телеком-інфраструктури.

Крім того, за допомогою програмно-визначених мереж та віртуальних мережевих функцій компанії спрощують конфігурацію та масштабування мереж, які стають все більш вимогливими до якості обслуговування (QoS). За даними аналітиків Sandvine, «важкий» контент відеосервісів та стрімінгових платформ становить 65% від всього інтернет-трафіку, а SDN та NFV ефективно його пріоритезують.

Водночас мережева віртуалізація скорочує операційні витрати. Замість того щоб витрачати час на налаштування пристроїв окремих постачальників, адміністратори керують потоком трафіку за допомогою API.

В індустрії можна зустріти думку, що мережева віртуалізація не виправдала очікувань. IP-мережі розробляли як стійке рішення, здатне функціонувати навіть при відмові окремих вузлів і ліній зв'язку. Але SDN та NFV, навпаки, централізують управління, що суперечить цій парадигмі. Якщо зловмиснику вдасться отримати доступ до серверів з керуючим ПЗ, він може перехопити контроль і проводити атаки типу «людина посередині».

Існує й інша проблема — керування віртуальними мережами відбувається за допомогою коду та API. Але тут, як і в будь-якому іншому програмному забезпеченні, можуть виникати помилки. Вони призводять до появи вразливостей і незапланованої поведінки інфраструктури. Однак справедливості заради варто зауважити, що існують способи підвищити безпеку SDN-екосистеми. Перш за все йдеться про багатофакторну аутентифікацію та регулярні аудити з метою пошуку некоректно налаштованих компонентів.

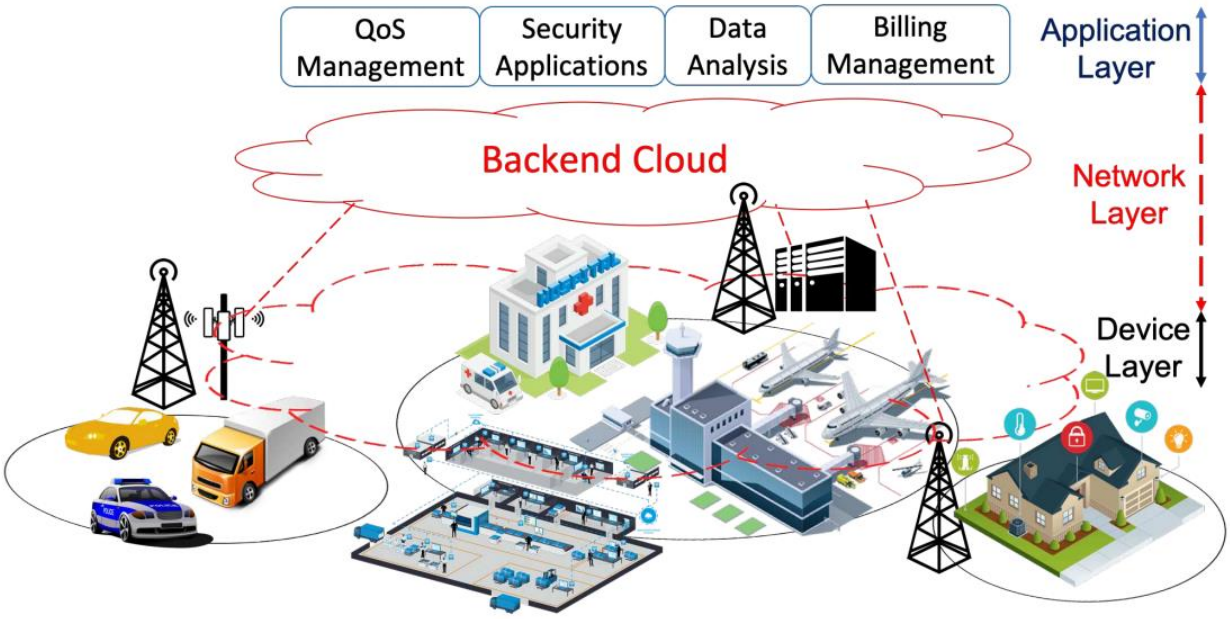



Рис. 1.5. Архітектура SDN-інтегрованого граничного обчислення

Хороший приклад — наше рішення для організації розподіленої мережевої інфраструктури Cloud SD-WAN, у якому є фізичний пристрій з функціями безпеки. Фактично це маршрутизатор, який може замінити вже розміщені у філіалах апаратні системи або працювати з ними в тандемі. Він підтримує функції мережевого шлюзу, Site-to-Site VPN, DHCP-сервера, NAT та брандмауера, а також різні протоколи маршрутизації для інтеграції з фізичною мережею.

Хмарний провайдер бере на себе всі завдання побудови інфраструктури SD-WAN. Це — налаштування політик безпеки, забезпечення інфраструктури та її цілодобовий моніторинг, адміністрування мережі та захищених розподілених ЦОД, виконання SLA. Водночас фахівці хмарного постачальника допомагають обрати оптимальне обладнання та дають рекомендації щодо модернізації мережі, щоб вона відповідала всім вимогам якості та надійності.

Якщо говорити про NFV, то технологія мала на меті спростити мережеву екосистему, але на практиці це явище не стало всеосяжним. При цьому сам по собі перехід на віртуальні мережі вимагає переосмислення інфраструктури та парадигми управління. Навіть велика компанія або інтернет-провайдер не може просто взяти та реалізувати стратегію з віртуалізації мережі. Міграція на SDN та NFV — це поступовий процес, але він не завжди призводить до бажаних

результатів. За статистикою експертів компанії Cloudify, провалюються 70% таких ініціатив.

Нарешті, не можна не відзначити, що багато рішень з віртуалізації будуються на вільному ПЗ. Однак для роботи з ними необхідна експертиза, зокрема для взаємодії з протоколами на кшталт OpenFlow, NETCONF, OVSDB.

### 1.5 Технології віртуалізації мережевих функцій

Віртуалізація мережевих функцій принесла безпрецедентну гнучкість у розгортанні та управлінні мережевими сервісами, однак породила серйозні проблеми з продуктивністю. Традиційні методи обробки мережевих пакетів через стек операційної системи демонструють значні обмеження пропускної здатності та збільшення затримок. Віртуалізація додає додатковий рівень абстракції, що призводить до втрат продуктивності через контекстні перемикання, емуляцію мережевого обладнання та подвійне копіювання пакетів. Ці обмеження стають критичними у вимогливих середовищах телекомунікаційних операторів, де необхідно обробляти мільйони пакетів на секунду.

Мережі п'ятого покоління висувають екстремальні вимоги до продуктивності мережевих функцій. Сервіси ультра-надійного зв'язку з малою затримкою (URLLC) вимагають часу відгуку менше 1 мс, тоді як розширена мобільна широкосмугова передача даних (eMBB) потребує пропускної здатності до 20 Гбіт/с. Критичні мережеві функції, такі як User Plane Function (UPF) та функції пакетного ядра, повинні обробляти трафік з мінімальними затримками та максимальною ефективністю. Ці вимоги неможливо задовольнити за допомогою традиційних методів віртуалізації, що необхідноє впровадження спеціалізованих технологій прискорення.

Для вирішення проблем продуктивності було розроблено низку технологій прискорення обробки мережевих пакетів. Data Plane Development Kit (DPDK) пропонує набір бібліотек для швидкої обробки пакетів у користувацькому просторі, обходячи повільний стек ядра ОС. Single Root I/O Virtualization (SR-IOV)

забезпечує прямий доступ віртуальних машин до мережевого обладнання, мінімізуючи накладні витрати гіпервізора. Open vSwitch (OVS) з підтримкою DPDK реалізує високошвидкісну віртуальну комутацію, інтегровану з архітектурою SDN. Кожна з цих технологій вирішує конкретні аспекти проблеми продуктивності та може використовуватися як окремо, так і в комбінації для досягнення оптимальних результатів.

Сучасний підхід до побудови високопродуктивних віртуалізованих мережевих інфраструктур передбачає комплексне використання декількох технологій прискорення. Комбінація DPDK для швидкої обробки пакетів, SR-IOV для мінімізації затримок доступу до мережевих інтерфейсів та оптимізованого OVS для ефективної віртуальної комутації дозволяє досягти продуктивності, порівнянної з виділеними апаратними рішеннями. Це особливо важливо для реалізації мережевих зрізів 5G, де різні сервіси мають суттєво відмінні вимоги до якості обслуговування, а ефективне використання ресурсів стає критичним фактором економічної доцільності.

DPDK (Data Plane Development Kit **)** або Комплект розробки площини даних**,** — це потужний інструмент, розроблений для підвищення продуктивності мережевих застосунків, забезпечуючи спрощену структуру для операцій площини даних. По суті, він дозволяє здійснювати пряме відображення пакетів з мережевих карт у простір користувача, минаючи ядро, для досягнення швидшої обробки. Ця можливість є критично важливою для компаній, які прагнуть створювати ефективні мережеві застосунки, такі як віртуалізовані сервіси. У цьому контексті VPP (векторна обробка пакетів) працює в просторі користувача та часто використовує DPDK як метод введення пакетів, діючи як застосунок, що використовує можливості DPDK для обробки пакетів.

У контексті віртуалізованих мережевих функцій (VNF) DPDK знаходить застосування для значного підвищення продуктивності критичних компонентів. Віртуальні маршрутизатори, балансувальники навантаження, межмережеві екрани та функції пакетного ядра 5G, реалізовані з використанням DPDK, демонструють продуктивність на рівні виділених апаратних рішень. Інтеграція DPDK з

платформами віртуалізації, такими як OpenStack або Kubernetes, дозволяє створювати високопродуктивні NFV-інфраструктури з підтримкою динамічного масштабування та міграції VNF між серверами.

DPDK відомий своїми надійними функціями, які задовольняють потреби високопродуктивних мереж:

Обробка пакетів у просторі користувача : Виконуючи операції в просторі користувача, DPDK зменшує затримку та підвищує пропускну здатність, уникаючи накладних витрат на простір ядра.

Драйвери режиму опитування (PMD) : ці драйвери постійно опитують мережеві інтерфейси на наявність вхідних пакетів, підвищуючи продуктивність, усуваючи необхідність переривань.

Розширене керування пам'яттю : DPDK включає механізми для ефективного керування пам'яттю, такі як великі сторінки пам'яті та пули пам'яті, оптимізуючи розподіл та звільнення буферів.

Масштабованість багатьох ядер : Розроблений для використання багатоядерних архітектур, DPDK дозволяє паралельну обробку даних на кількох ядрах, значно підвищуючи продуктивність.

Підтримка кількох мережевих карт : підтримує широкий спектр мережевих карт від різних постачальників, що забезпечує адаптивність до різних середовищ.

Гнучка платформа обробки пакетів : DPDK надає бібліотеки для обробки пакетів як без збереження стану, так і з утриманням стану, що дозволяє розробляти власні мережеві програми.

Висока пропускна здатність та низька затримка : Зосереджений на оптимізації продуктивності, DPDK досягає високої пропускної здатності, мінімізуючи затримку, що є важливим для телекомунікаційних та хмарних сервісів.

Багата екосистема : Завдяки активній спільноті та численним бібліотекам, що додаються, функціональність DPDK постійно вдосконалюється, що спрощує його використання в різних сценаріях.

Відкритий код : Як проект з відкритим кодом, DPDK дозволяє розробникам змінювати та вдосконалювати код, забезпечуючи постійні оновлення та покращення функцій.

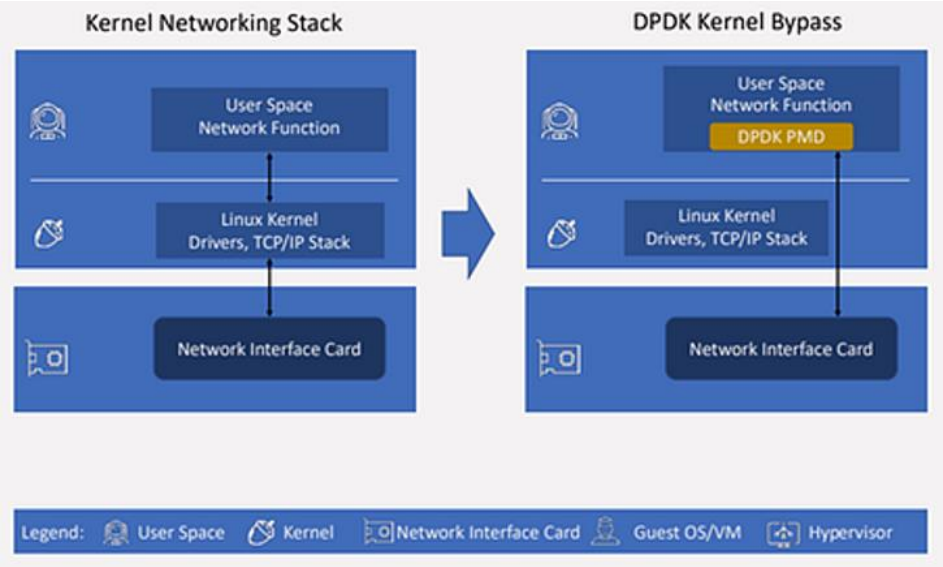



Рис. 1.6. Комплект розробки площини даних

Ці функції роблять DPDK ідеальним вибором для програм, що потребують швидкої та ефективної обробки пакетів, таких як маршрутизатори, брандмауери та інші мережеві пристрої.

Серед основних обмежень DPDK можна відзначити високу складність розробки та налагодження програм, необхідність глибоких знань архітектури апаратного забезпечення, та обмежену сумісність з існуючим програмним забезпеченням, розробленим для традиційного мережевого стека. Використання DPDK вимагає виділення виділених ядер процесора для обробки пакетів, що може знижувати загальну ефективність використання ресурсів сервера. Крім того, постійна розробка нових версій та необхідність адаптації до змін у апаратних платформах створює додаткові виклики для підтримки рішень на основі DPDK у довгостроковій перспективі.

Single Root I/O Virtualization (SR-IOV) є специфікацією промислового стандарту, розробленою консорціумом PCI-SIG, яка дозволяє одному фізичному пристрою Peripheral Component Interconnect Express (PCIe) представляти себе як кілька незалежних віртуальних пристроїв. Ця технологія була спеціально

розроблена для забезпечення ефективної віртуалізації мережевих інтерфейсів у серверних середовищах. Стандарт SR-IOV визначає архітектурні принципи та інтерфейси, що дозволяють розподіляти ресурси фізичного мережевого адаптера між численними віртуальними машинами без значного зниження продуктивності.

Архітектура SR-IOV базується на розподілі ресурсів фізичного мережевого адаптера між кількома віртуальними середовищами. Ключовим компонентом є PCIe Root Complex, який забезпечує взаємодію між процесором, пам'яттю та PCIe пристроями. Архітектура включає механізми ізоляції пам'яті, віртуалізації DMA-транзакцій та управління подіями. Спеціалізовані апаратні засоби на самому мережевому адаптері забезпечують ефективний розподіл пропускної здатності та обробку мережевих пакетів для кожного віртуального інтерфейсу.

Основним елементом архітектури SR-IOV є поділ на Фізичні функції (Physical Functions - PF) та Віртуальні функції (Virtual Functions - VF). PF представляє повнофункціональний PCIe функцію, яка має повний контроль над пристроєм і відповідає за управління та конфігурацію всього адаптера. VF є спрощеними "легкими" функціями, що надають лише базові можливості для роботи з мережею. Кожна VF має власні ресурси, включаючи MAC-адреси, таблиці MAC/VLAN, та черги передачі/прийому, що забезпечує повну ізоляцію між різними віртуальними середовищами.

SR-IOV забезпечує прямий доступ віртуалізованих мережевих функцій (VNF) до апаратних ресурсів мережевого адаптера, мінімізуючи участь гіпервізора в обробці мережевого трафіку. Кожна VF може бути безпосередньо призначена віртуальній машині через механізм PCIe Passthrough, що дозволяє VNF працювати з мережевим адаптером як з виділеним фізичним пристроєм. Це усуває необхідність емуляції мережевого обладнання та значно знижує накладні витрати, пов'язані з копіюванням пакетів між адресними просторами гіпервізора та віртуальної машини.

У контексті мереж 5G SR-IOV демонструє значний позитивний вплив на продуктивність критичних мережевих функцій. Технологія дозволяє досягти затримок обробки пакетів на рівні 10-20 мікросекунд, що є критично важливим для сервісів ультра-надійного зв'язку з малою затримкою (URLLC). Пропускна

здатність мережевих інтерфейсів може досягати лінійної швидкості (до 100 Гбіт/с та вище) на кожній VF, забезпечуючи ефективну підтримку сервісів розширеної мобільної широкосмугової передачі даних (eMBB).

Незважаючи на значні переваги, SR-IOV має певні обмеження. Технологія вимагає спеціалізованого апаратного забезпечення з підтримкою SR-IOV та може ускладнити міграцію віртуальних машин між фізичними серверами. Крім того, обмежена кількість VF на одному адаптері (зазвичай до 64-256) може створювати обмеження для масштабування. Для ефективного використання SR-IOV необхідна ретельне планування інфраструктури та спеціалізовані інструменти управління, що додає складності в експлуатацію віртуалізованих мережевих середовищ.

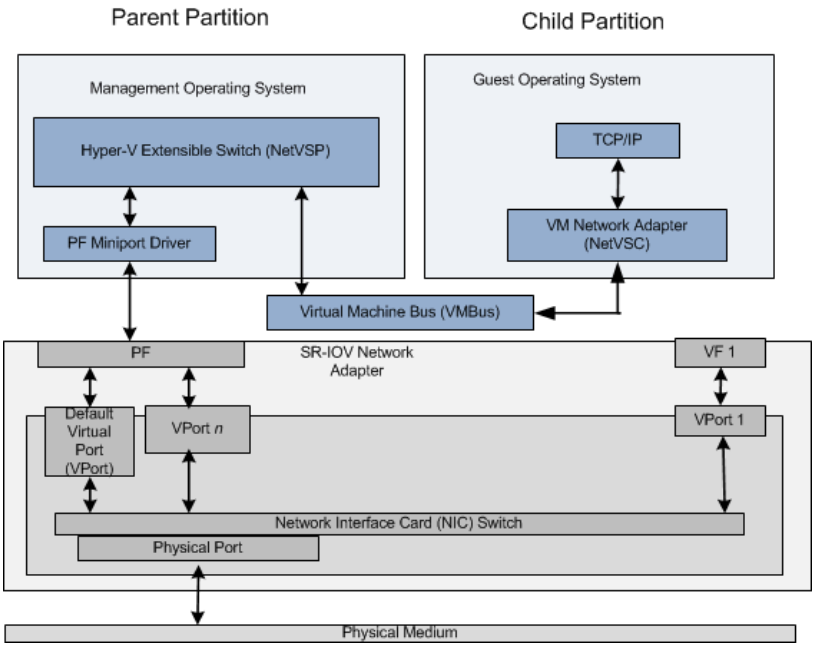



Рис. 1.7. Інтерфейс SR-IOV

Архітектура SR-IOV в середовищі Hyper-V базується на взаємодії кількох ключових компонентів. Центральним елементом є модуль розширюваного комутатора Hyper-V, який налаштовує комутатор мережевого інтерфейсу на адаптері SR-IOV для забезпечення підключення віртуальних машин. Фізична функція (PF) представляє повноцінну функцію PCIe адаптера і відповідає за управління ресурсами SR-IOV, тоді як драйвер мініпорту PF забезпечує керування цими ресурсами з рівня операційної системи. Важливою особливістю є те, що при

прямому підключенні віртуальної машини до віртуальної функції (VF) трафік даних передається без участі модуля комутатора, що значно підвищує продуктивність.

Віртуалізовані компоненти та їх взаємодія включають віртуальні функції (VF) - спрощені функції PCIe, які представляють віртуалізовані екземпляри мережного адаптера. Кожна VF керується драйвером мініпорту VF, встановленим у віртуальній машині, що забезпечує ізоляцію операцій між різними VF. Апаратний комутатор мережного адаптера (NIC Switch) перенаправляє трафік між фізичним портом адаптера та віртуальними портами (VPorts), кожен з яких підключений до PF або VF. Фізичний порт забезпечує з'єднання з зовнішнім мережевим середовищем, завершуючи архітектуру, що дозволяє ефективно розподіляти ресурси одного фізичного адаптера між численними віртуальними середовищами.

Open vSwitch (OVS) є розподіленим віртуальним комутатором з відкритим кодом, призначеним для забезпечення мережевого зв'язку в багатокористувацьких середовищах віртуалізації. Архітектура OVS складається з ядра комутатора, що працює в просторі ядра операційної системи, та користувацького демона ovs-vswitchd, який керує логікою комутації. Ключовим компонентом є база даних OVSDB, що зберігає конфігурацію комутатора та стан мережних інтерфейсів. Архітектура підтримує розподілене виконання, дозволяючи створювати складні мережні топології з кількома екземплярами OVS, що взаємодіють між собою.

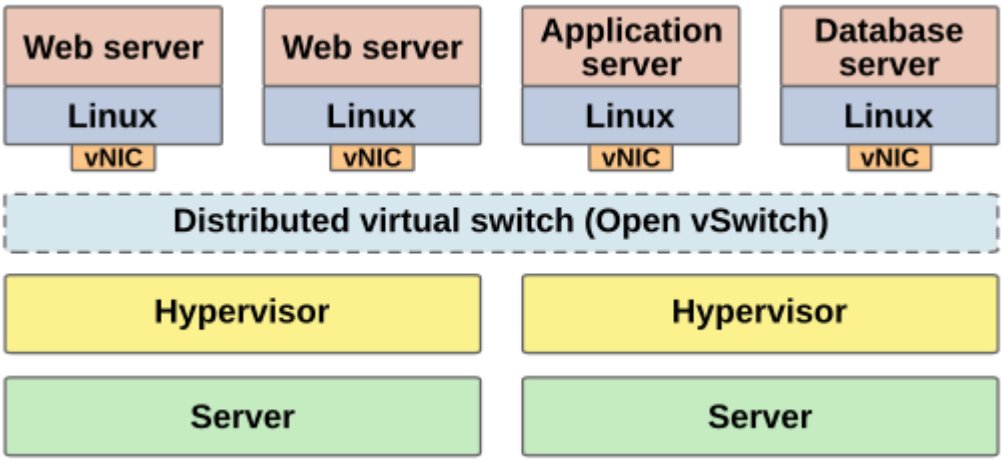



Рис. 1.8. Міжсерверний віртуальний мережевий комутатор Open vSwitch

OVS глибоко інтегрований з архітектурою SDN через підтримку протоколу OpenFlow. Комутатор може працювати в кількох режимах: як автономний комутатор з власною логікою маршрутизації, або як керований комутатор під контролем зовнішнього SDN-контролера. Через протокол OpenFlow версії 1.0-1.5 контролер може динамічно додавати, змінювати та видаляти правила в таблицях потоків OVS. Ця інтеграція дозволяє реалізувати складні мережні політики, балансування навантаження та механізми безпеки на рівні всієї мережної інфраструктури.

Основним механізмом обробки трафіку в OVS є система таблиць потоків, організованих у конвеєр обробки пакетів. Кожна таблиця потоків містить набір правил, що складаються з полів відповідності (match fields), пріоритетів, лічильників та дій. Поля відповідності можуть включати MAC-адреси, IP-адреси, порти TCP/UDP, VLAN теги та метадані. Дії можуть включати перенаправлення на конкретний порт, модифікацію заголовків пакетів, відкидання пакету або переходу до наступної таблиці. Конвеєрна архітектура дозволяє реалізувати складну логіку обробки трафіку з мінімальними затримками.

У хмарних середовищах та інфраструктурі віртуалізації мережевих функцій (NFVI) OVS відіграє ключову роль як основний віртуальний комутатор. Він інтегрований з провідними платформами віртуалізації, включаючи OpenStack, Kubernetes та VMware. В OpenStack Neutron OVS забезпечує реалізацію мережевих сервісів, таких як віртуальні мережі, підмережі, маршрутизатори та групи безпеки. У контексті NFVI OVS забезпечує комутацію між віртуалізованими мережевими функціями (VNF), дозволяючи створювати складні ланцюги обслуговування (service chains) для обробки мережного трафіку.

OVS надає розвинені інструменти моніторингу та управління мережевим трафіком. Через інтерфейс OVSDB адміністратори можуть отримувати детальну статистику по портах, потоках та інтерфейсах. Підтримка протоколу sFlow дозволяє здійснювати вибірковий збір даних про трафік для аналізу продуктивності мережі. Інструменти на кшталт ovs-ofctl та ovs-appctl забезпечують низькорівневий контроль над конфігурацією комутатора та потоків. Для відладки складних

мережних конфігурацій OVS надає механізм трасування шляху пакетів (tracing), що дозволяє моделювати обробку пакетів через конвеєр таблиць потоків.

Для забезпечення високої продуктивності в середовищах з інтенсивним мережевим навантаженням OVS підтримує інтеграцію з технологією DPDK. OVS з DPDK дозволяє обробляти мережеві пакети в користувацькому просторі, обходячи повільний стек ядра Linux. Це забезпечує значно вищу пропускну здатність (до 100 Гбіт/с та вище) та знижує затримки обробки пакетів. Спеціалізовані polling-драйвери DPDK замінюють традиційні переривання, що дозволяє досягти детермінованої продуктивності, критично важливої для реальних застосунків у телекомунікаційних мережах 5G.

Аналіз технологій віртуалізації мережевих функцій виявив чіткі конкурентні переваги кожної з розглянутих технологій. DPDK демонструє найвищу ефективність у сценаріях, що вимагають інтенсивної програмної обробки пакетів, завдяки повному обходу мережевого стека ядра ОС та оптимізованому використанню апаратних ресурсів. SR-IOV забезпечує мінімальні затримки та максимальну пропускну здатність шляхом надання прямих апаратних функцій віртуальним машинам, що робить її ідеальним рішенням для роботи з високошвидкісними мережевими інтерфейсами. OVS пропонує неперевершену гнучкість управління мережевими потоками та інтеграцію з архітектурою SDN, будучи стандартом де-факто для побудови складних віртуальних мереж у хмарних середовищах.

Перспективи розвитку досліджуваних технологій пов'язані з подальшою оптимізацією продуктивності та інтеграцією з новими апаратними платформами. Для DPDK це передбачає розширення підтримки програмованих мережевих пристроїв (SmartNIC) та інтеграцію з фреймворками машинного навчання для адаптивної оптимізації продуктивності. SR-IOV розвивається у напрямку підвищення масштабованості та підтримки динамічного перерозподілу віртуальних функцій між різними користувачами. Найбільший потенціал для OVS полягає в подальшій інтеграції з технологіями контейнеризації, розвитку

механізмів автоматичного налаштування та вдосконаленні інструментів моніторингу для забезпечення сквозної observability в розподілених системах.

Вибір оптимальної технології або їх комбінації повинен ґрунтуватися на конкретних вимогах до продуктивності, масштабованості та гнучкості. Для критичних сервісів URLLC з вимогами до затримки менше 1 мс рекомендується SR-IOV у поєднанні з виділеними апаратними ресурсами. Для сервісів eMBB з високими вимогами до пропускної здатності оптимальним рішенням є комбінація OVS з DPDK для програмованої комутації та SR-IOV для прискорення доступу до мережі. У сценаріях mMTC з великою кількістю підключень та обмеженим трафіком ефективним рішенням буде OVS з традиційними драйверами ядра для забезпечення балансу між продуктивністю та щільністю підключень. Для гнучкого управління мережевими зрізами рекомендується комбіноване використання всіх трьох технологій з централізованим оркеструванням через SDN-контролер.

### 1.6 Аналіз платформ з відкритим кодом: OpenStack як NFVI, ONAP

Відкриті платформи відіграють вирішальну роль у трансформації телекомунікаційних систем, забезпечуючи необхідну гнучкість, інноваційність та економічну ефективність для розгортання мереж 5G. Відкритий код дозволяє операторам уникати вендорного блокування, прискорювати розробку нових сервісів та адаптувати рішення під специфічні вимоги, що особливо важливо в умовах динамічного розвитку телекомунікаційних стандартів і сервісів.

Сучасні платформи для впровадження NFV/SDN повинні забезпечувати повний стек функціоналу - від віртуалізації інфраструктури до оркестрації сервісів, що реалізовано в провідних open-source проєктах. Серед них OpenStack як основа NFVI, ONAP для автоматизації мережевих сервісів, Kubernetes для контейнеризації мережевих функцій, а також спеціалізовані рішення типа OpenDaylight та Tungsten Fabric для реалізації SDN-архітектури в масштабованих середовищах 5G.

OpenStack як NFVI представляє модульну хмарну платформу, що складається з взаємопов'язаних компонентів. Ключові сервіси включають Nova для обчислювальних ресурсів, Neutron для мережевих функцій, Cinder для блочного сховища та Glance для управління образами. Архітектура заснована на мікросервісному підході з API-орієнтованими інтерфейсами, що забезпечує гнучкість і масштабованість. Кожен компонент функціонує незалежно, але інтегрується через єдині стандартизовані API, що дозволяє створювати комплексну інфраструктуру для розгортання VNF.

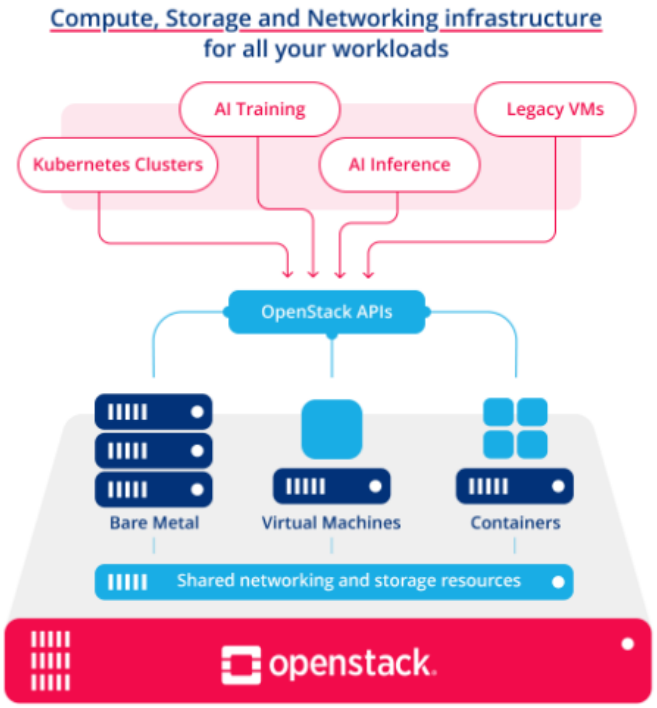



Рис. 1.9. Панелі інструментів OpenStack

Neutron як основний мережевий компонент OpenStack надає розширені можливості для NFV, включаючи управління віртуальними мережами, підмережами та портами. Модуль підтримує створення розподілених віртуальних маршрутизаторів (DVR), мережевих функцій як сервісу (NFaaS) та механізми безпеки. Для NFV критично важливими є можливості Neutron щодо підтримки VLAN, VXLAN та Geneve тунелювання, що забезпечує необхідну ізоляцію та гнучкість мережевих конфігурацій для різних VNF.

OpenStack інтегрується з провідними технологіями віртуалізації для забезпечення високої продуктивності NFVI. Підтримка KVM як гіпервізора забезпечує ефективну віртуалізацію апаратних ресурсів. Інтеграція з DPDK дозволяє прискорити обробку мережевих пакетів, а SR-IOV забезпечує прямий доступ до фізичних мережевих інтерфейсів. Ця комбінація технологій дозволяє досягти продуктивності, необхідної для критичних мережевих функцій 5G.

Nova як обчислювальний модуль забезпечує динамічне виділення ресурсів CPU та RAM для VNF, підтримуючи live-міграцію та автоматичне масштабування. Cinder надає персистентні сховища даних з підтримкою різних бекендів (CEPH, iSCSI, FC), що критично важливо для збереження стану мережевих функцій. Оптимальна конфігурація цих компонентів забезпечує високу доступність та продуктивність VNF у відповідності до вимог телеком-навантажень.

OpenStack забезпечує розширену підтримку мережевих зрізів через інтеграцію з проектами типу Dragonflow та Neutron QoS. Механізми якості обслуговування дозволяють гарантувати пропускну здатність, обмежувати трафік та пріоритезувати потоки для різних типів сервісів. Це особливо важливо для реалізації різних категорій сервісів 5G - від масивних IoT-підключень до сервісів з ультра-низькою затримкою.

Tacker є оркестратором мережевих функцій з відкритим кодом, розробленим як компонент OpenStack. Архітектура включає модуль VNF Manager (VNFM) для керування віртуалізованими мережевими функціями та NFV Orchestrator (NFVO) для оркестрації ресурсів. Головне призначення Tacker - автоматизація розгортання, масштабування та моніторингу VNF на основі політик, визначених оператором.

Tacker забезпечує повний життєвий цикл VNF, включаючи ініціалізацію, встановлення, масштабування, оновлення та завершення роботи. Модуль підтримує автоматичне масштабування на основі метрик навантаження, health-моніторинг та самовідновлення у разі збоїв. Це дозволяє забезпечити високу доступність мережевих сервісів та ефективно керувати ресурсами інфраструктури.

Tacker реалізує стандарти ETSI NFV SOL, забезпечуючи сумісність з промисловими вимогами. Підтримка стандартних дескрипторів VNF (VNFD) та

мережевих сервісів (NSD) дозволяє використовувати готові шаблони для швидкого розгортання сервісів. Впровадження відкритих стандартів спрощує інтеграцію з різними вендорськими рішеннями та забезпечує інтероперабельність у багатовендорних середовищах.

Tacker інтегрується з різними VIM, включаючи OpenStack, Kubernetes та VMware, через стандартизовані API. Ця інтеграція дозволяє керувати ресурсами NFVI незалежно від базової платформи, забезпечуючи уніфіковане управління в гетерогенних середовищах. Підтримка мульти-вім дозволяє розподіляти VNF між різними центрами обробки даних, що критично важливо для створення відмовостійкої архітектури мереж 5G.

ONAP (Open Network Automation Platform) являє собою комплексну платформу з модульною архітектурою, спрямовану на автоматизацію телекомунікаційних мереж. Архітектура платформи поділяється на два основних рівні: рівень дизайну (Design Framework) та рівень виконання (Execution Framework). До ключових компонентів належать Service Orchestrator (SO), який координує створення та управління сервісами, Active and Available Inventory (A&AI), що забезпечує реальний інвентар ресурсів і сервісів, а також Policy Framework для управління політиками. ONAP також включає компоненти моніторингу та аналітики, такі як DCAE (Data Collection, Analytics and Events), які забезпечують збір даних про стан мережі в реальному часі.

ONAP реалізує модель керування життєвим циклом сервісів, що охоплює всі етапи — від проектування до виведення з експлуатації. Процес починається з фази дизайну, де описуються сервіси, ресурси та політики за допомогою інструментів, таких як SDC (Service Design and Creation). Після цього відбувається оркестрація розгортання сервісу через Service Orchestrator, який взаємодіє з інфраструктурою (VIM, SDN контролери) для виділення необхідних ресурсів. Під час експлуатації ONAP забезпечує моніторинг, масштабування та оновлення сервісів, а також автоматичне виявлення та усунення несправностей через механізми закритого циклу управління.

ONAP забезпечує оркестрацію сервісів на основі моделей (model-driven), що дозволяє автоматизувати складні процеси в багатовендорних середовищах. Платформа використовує архітектуру, що підтримує декілька оркестраторів (мульти-вім), для управління різними технологічними доменами, такими NFVI, MEC та транспортні мережі. ONAP також інтегрується з системами управління (EMS, NMS) та обладнанням різних виробників через адаптери, що забезпечує автоматизацію крос-доменних операцій. Це дозволяє, наприклад, автоматично створювати мережеві зрізи (network slices) або переналаштовувати маршрутизацію трафіку відповідно до змінних умов.

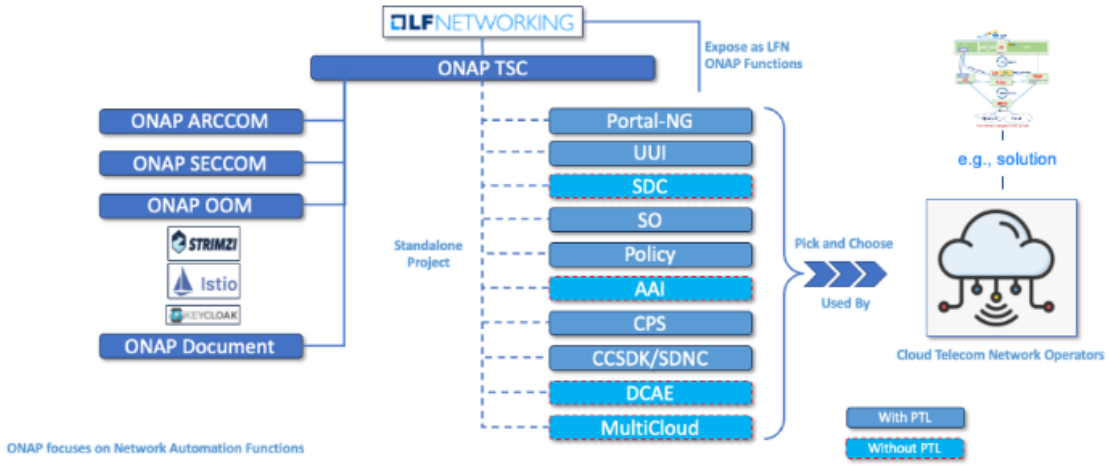



Рис. 1.10 Організаційна схема ONAP

Критично важливою особливістю ONAP є підтримка політиково-орієнтованого управління (Policy-Driven Orchestration) і закритого циклу (Closed-Loop Automation). Policy Framework дозволяє визначати правила та політики, які автоматично застосовуються для управління сервісами та ресурсами. Наприклад, політика може визначати умови для масштабування VNF або перенаправлення трафіку при виявленні перевантаження. Замкнутий цикл управління, реалізований через інтеграцію DCAE та Policy Framework, дозволяє автоматично виявляти аномалії (наприклад, зростання затримки) і запускати коригувальні дії без участі оператора, забезпечуючи високу адаптивність і ефективність мережі 5G.

OpenStack та ONAP знаходять комплексне застосування в різних компонентах архітектури 5G. OpenStack як NFVI-платформа використовується для розгортання

віртуалізованих функцій ядра 5G Core, таких як AMF, SMF та UPF, забезпечуючи їх ізоляцію та масштабованість. ONAP відповідає за оркестрацію складних сервісів, наприклад, послідовностей обробки трафіку (service chains) між різними VNF. Для роботи з контейнеризованими мережевими функціями (CNF) OpenStack інтегрується з Kubernetes через плагіни (наприклад, Magnum або Kuryr), що дозволяє керувати контейнерами як обчислювальним ресурсом. ONAP, у свою чергу, забезпечує життєвий цикл CNF, використовуючи моделі розгортання та політики, аналогічні до VNF.

Керування мережевими зрізами (network slicing) є одним з ключових сценаріїв використання ONAP у 5G. ONAP дозволяє проектувати, оркеструвати та моніторити окремі зрізи для різних сервісів (eMBB, URLLC, mMTC) на основі єдиної фізичної інфраструктури. Він автоматизує виділення ресурсів (обчислень, мережі, сховища) для кожного зрізу через інтеграцію з OpenStack (як VIM). OpenStack забезпечує ізоляцію ресурсів на інфраструктурному рівні, створюючи окремі мережі, обчислювальні кластери та правила безпеки для різних зрізів. Разом ці платформи забезпечують енд-ту-енд управління зрізом — від радіочастотної частини (RAN) до ядра мережі.

Таблиця 1.1

Порівняння OpenStack та ONAP

| **Критерій порівняння** | **OpenStack** | **ONAP** |
|---|---|---|
| Основна функція | Інфраструктура віртуалізації (NFVI) | Оркестрація та автоматизація сервісів |
| Архітектурна роль | Віртуалізована інфраструктура (VIM) | Оркестратор верхнього рівня |
| Робота з контейнерами | Інтеграція з Kubernetes (Magnum, Kuryr) | Управління CNF через моделі розгортання |
| Механізми доступності | Live Migration, резервування екземплярів | Політики закритого циклу, автоматичне відновлення |

| **Критерій порівняння** | **OpenStack** | **ONAP** |
|---|---|---|
| Моніторинг та аналітика | Базовий моніторинг ресурсів | Розширена аналітика через DCAE |
| Масштабованість | Вертикальне масштабування окремих компонентів | Горизонтальне масштабування сервісів |
| Складність розгортання | Висока (потрібна конфігурація багатьох компонентів) | Дуже висока (складна архітектура) |
| Підтримка політик | Обмежена (QoS, безпека) | Розширена (Policy Framework) |
| Типовий час розгортання | Години-дні (залежить від складності) | Дні-тижні (для повної інтеграції) |
| Екосистема | Велика спільнота, багато драйверів | Спеціалізована для телекомунікацій |
| Вимоги до ресурсів | Високі (мінімум 3 сервери для production) | Дуже високі (потрібні додаткові сервери для аналітики) |

Для досягнення високої доступності, необхідної для критичних сервісів 5G, OpenStack надає механізми резервування, Live Migration та автоматичного відновлення екземплярів VNF. ONAP доповнює ці можливості на рівні сервісу, реалізуючи політики закритого циклу управління. Наприклад, при виявленні збою у роботі UPF через аналітику в реальному часі (DCAE), ONAP автоматично ініціює перерозподіл навантаження або розгортання резервної VNF. Спільна робота цих платформ дозволяє забезпечити дотримання SLA, мінімізувати час простою та ефективно керувати ресурсами для підтримки надійності всієї мережевої інфраструктури 5G.

# 2. ОЦІНКА ЕФЕКТИВНОСТІ ТЕХНОЛОГІЙ МЕРЕЖЕВОЇ ВІРТУАЛІЗАЦІЇ В SDN/NFV-ІНФРАСТРУКТУРІ 5G

## 2.1 Формулювання цілей та критеріїв оцінки ефективності

При обґрунтованій оцінці ефективності провідних технологій мережевої віртуалізації, включаючи DPDK, SR-IOV та Open vSwitch, у контексті їх застосування в SDN/NFV-інфраструктурі мереж 5G необхідно приділити увагу розробці цілісної методики оцінки, яка враховує специфічні вимоги до продуктивності різних сервісних категорій 5G.

Основним стратегічним завданням є розробка комплексної методики оцінки ефективності технологій мережевої віртуалізації для SDN/NFV-інфраструктури 5G. Дослідження спрямоване на визначення оптимальних співвідношень між продуктивністю, вартістю та енергоефективністю різних технологічних рішень. Ключовою метою є створення уніфікованої системи критеріїв, що дозволить порівнювати ефективність технологій віртуалізації в різних сценаріях використання мереж 5G.

Для оцінки продуктивності використовуються критерії пропускної здатності, затримки та втрат пакетів. Пропускна здатність вимірюється в Гбіт/с для різних типів трафіку, включаючи TCP та UDP потоки. Затримка аналізується на рівні мікросекунд для критичних додатків URLLC, зокрема вимірюються затримки між різними компонентами віртуалізованої інфраструктури. Втрати пакетів оцінюються при різних рівнях навантаження для виявлення граничних можливостей системи.

Критерії масштабованості та еластичності

Масштабованість оцінюється через здатність системи обробляти зростаюче навантаження без погіршення якості обслуговування. Аналізується максимальна кількість одночасних підключень, кількість оброблених потоків даних та динаміка продуктивності при збільшенні кількості VNF. Еластичність визначається швидкістю масштабування ресурсів відповідно до змін навантаження, включаючи час розгортання нових екземплярів VNF та перерозподіл навантаження між ними.

Ефективність використання ресурсів

Ця група критеріїв включає використання процесорних ресурсів (CPU), оперативної пам'яті та мережевих інтерфейсів. Вимірюється співвідношення продуктивності до споживаних ресурсів, що дозволяє оцінити економічну ефективність рішень. Особлива увага приділяється аналізу ефективності використання ресурсів при різних технологіях віртуалізації та їх впливу на загальну продуктивність системи.

Енергоефективність та експлуатаційні витрати

Енергоефективність оцінюється через споживання енергії на одиницю обробленого трафіку. Аналізуються експлуатаційні витрати, включаючи вартість обладнання, енергоспоживання та обслуговування інфраструктури. Враховуються як прямі, так і непрямі витрати, пов'язані з управлінням та підтримкою роботи віртуалізованої інфраструктури.

Надійність та доступність

Критерії надійності включають час безвідмовної роботи системи, середній час відновлення після збоїв та стійкість до відмов окремих компонентів. Доступність оцінюється через відсоток часу роботи системи (uptime) та здатність забезпечувати безперервність сервісів при виході з ладу окремих елементів інфраструктури.

Безпека та ізоляція

Аналізується здатність системи забезпечувати ізоляцію між різними мережевими зрізами та віртуальними мережами. Оцінюється рівень безпеки при використанні різних технологій віртуалізації, включаючи захист від несанкціонованого доступу та забезпечення конфіденційності даних. Особлива увага приділяється аналізу вразливостей, пов'язаних із централізацією управління в SDN-архітектурі.

Інтеграція та сумісність

Ця група критеріїв оцінює здатність технологій віртуалізації інтегруватися з існуючою інфраструктурою та сумісність з різними апаратними платформами. Аналізується простота інтеграції нових рішень, підтримка стандартних протоколів

та інтерфейсів, а також можливість створення гетерогенних середовищ з різними технологіями віртуалізації.

### 2.2. Вибір типових сценаріїв роботи 5G-мережі (eMBB, uRLLC, mMTC).

Сучасні мережі п'ятого покоління (5G) представляють собою не єдину універсальну технологію, а скоріше комплексну екосистему, здатну адаптуватися до різноманітних вимог сервісів та застосунків. На відміну від попередніх поколінь, архітектура 5G була концептуально розроблена для одночасної підтримки широкого спектру послуг з принципово різними характеристиками – від надшвидкісних потокових трансляцій до критично важливих систем автоматизації. Ця унікальна здатність реалізується через три фундаментальні категорії сервісів, що визначають логіку функціонування всієї мережевої інфраструктури.

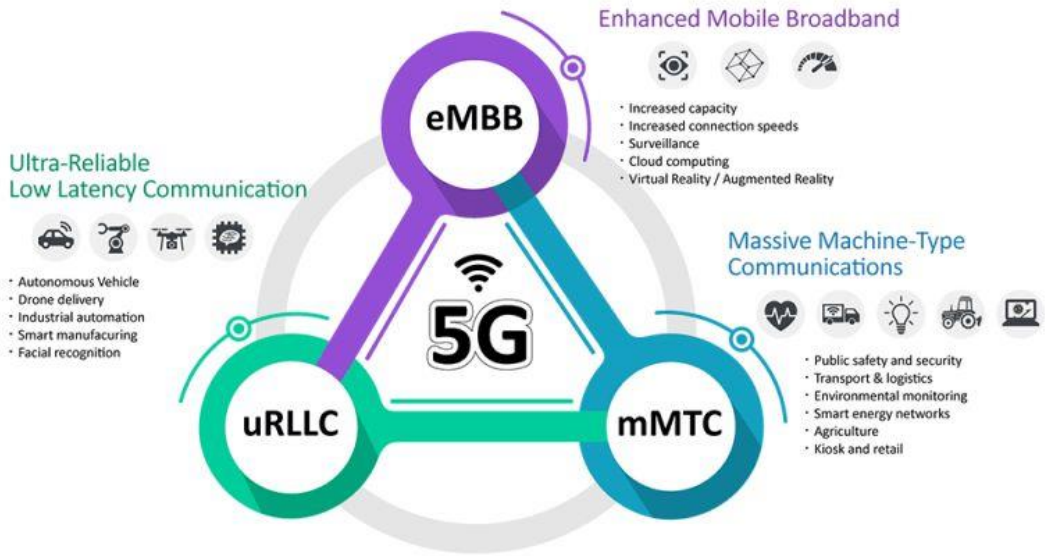



Рис. 2.1. Сценаріїв роботи 5G-мережі

Вибір сценаріїв eMBB (розширена мобільна широкосмуговість), uRLLC (надійний зв'язок з ультра-низькою затримкою) та mMTC (масивний зв'язок між машинами) як об'єктів дослідження обумовлений їх ключовою роллю у формуванні вимог до мережевої інфраструктури. Кожен з цих сценаріїв представляє не лише технічні характеристики, але цілі бізнес-моделі та споживчі очікування, що в

сукупності охоплюють понад 90% прогнозованих варіантів використання мереж 5G. Аналіз саме цих трьох напрямів дозволяє створити комплексне уявлення про ефективність роботи всієї мережі в цілому.

Проведення оцінки технологій мережевої віртуалізації окремо для кожної категорії сервісів є критично важливим етапом дослідження, оскільки дозволяє виявити специфічні вимоги до продуктивності, надійності та масштабованості для кожного типу навантаження. Такий підхід забезпечує отримання об'єктивних даних для прийняття обґрунтованих рішень щодо вибору архітектурних рішень та технологій віртуалізації при проектуванні та оптимізації мережевої інфраструктури 5G.

eMBB (enhanced Mobile Broadband – розширена мобільна широкосмуговість.

eMBB є одним з трьох фундаментальних сценаріїв використання мереж 5G, орієнтованим на забезпечення високошвидкісного доступу до мультимедійного контенту та інтерактивних сервісів. Цей напрям розроблений для задоволення зростаючих потреб користувачів у передачі великих обсягів даних із мінімальними обмеженнями щодо пропускної здатності. Основна відмінність eMBB від інших сценаріїв полягає в акценті на максимальну швидкість передачі даних при збереженні стабільної якості обслуговування.

До ключових застосувань eMBB належать стрімінг відеоконтенту у високій роздільній здатності (4K/8K), що вимагає стабільного каналу зв'язку з пропускною здатністю до 50 Мбіт/с для одного потоку. Технології віртуальної та доповненої реальності (VR/AR) використовують eMBB для передачі об'ємних даних у реальному часі, забезпечуючи імерсивний досвід користувача. Також сценарій включає швидке завантаження великих файлів, інтерактивні онлайн-ігри з високою графікою та роботу з хмарними сервісами, де необхідна миттєва передача значних обсягів інформації.

Для ефективної реалізації eMBB необхідно забезпечити пікову швидкість передачі даних до 20 Гбіт/с у нисхідному потоці та 10 Гбіт/с у上行ому. Затримка в мережі не повинна перевищувати 10 мс для більшості додатків, хоча для інтерактивних сервісів рекомендується значення до 4-5 мс. Щільність підключення

становить до 100 000 пристроїв на км² у щільноміських умовах. Критично важливим є забезпечення високої спектральної ефективності та підтримка технології масивного MIMO.

Для обробки трафіку eMBB технології віртуалізації повинні забезпечувати ефективне використання мережевих ресурсів та обробку великих потоків даних. DPDK дозволяє досягти високої пропускної здатності шляхом оптимізації обробки пакетів у користувацькому просторі. SR-IOV забезпечує прямий доступ до мережевих інтерфейсів, мінімізуючи затримки при передачі великих обсягів даних. Open vSwitch з підтримкою DPDK дозволяє ефективно керувати мережевими потоками та забезпечувати якість обслуговування (QoS) для різних категорій трафіку.

Оцінка ефективності технологій віртуалізації для eMBB проводиться шляхом вимірювання пропускної здатності при різних типах навантаження, включаючи передачу великих файлів, потокове відео високої роздільної здатності та інтерактивні VR/AR-додатки. Аналізується залежність продуктивності від кількості одночасних підключень, ефективність використання ресурсів ЦП та пам'яті, а також здатність системи підтримувати стабільну якість обслуговування при зростанні навантаження. Особлива увага приділяється вимірюванню затримок у віртуалізованій інфраструктурі та їх впливу на якість користувацького досвіду.

uRLLC (Ultra-Reliable and Low-Latency Communications) - надійний зв'язок з ультра-низькою затримкою

uRLLC  сценарій використання мереж 5G, орієнтований на додатки, де найвищі вимоги висуваються до надійності зв'язку та мінімізації затримок передачі даних. Цей сценарій передбачає гарантовану доставку даних із затримкою менше 1 мс та надійністю на рівні 99.999%. Такі характеристики роблять uRLLC критично важливим для систем, де будь-яка затримка чи втрата даних може призвести до серйозних наслідків.

uRLLC знаходить застосування в галузях, що вимагають миттєвого реагування та високої надійності. До ключових прикладів належать: безпілотні транспортні засоби, що потребують миттєвого обміну даними для уникнення аварій;

телемедицина, зокрема дистанційні хірургічні операції; промислова автоматизація та "доторкніться до мене" (tactile internet) для керування роботизованими системами; автоматизація енергосистем для швидкого реагування на зміни навантаження; та системи допомоги водію в реальному часі.

Для реалізації uRLLC необхідно забезпечити затримку менше 1 мс при надійності зв'язку 99.999%. Це вимагає впровадження технологій міліметрових хвиль (mmWave) для зменшення часу передачі, мережевої нарізки (network slicing) для ізоляції критичного трафіку, та edge computing для розміщення обчислювальних ресурсів ближче до кінцевих користувачів.

Для uRLLC технології віртуалізації повинні забезпечувати мінімальні затримки обробки даних. SR-IOV стає ключовою технологією для прямих апаратних підключень, що усуває затримки гіпервізора. DPDK дозволяє оптимізувати обробку пакетів, а спеціалізовані версії Open vSwitch забезпечують детерміновану маршрутизацію. Оцінка ефективності включає вимірювання затримок між різними компонентами віртуалізованої інфраструктури, аналіз стабільності роботи при тривалому навантаженні та тестування механізмів відновлення після збоїв.

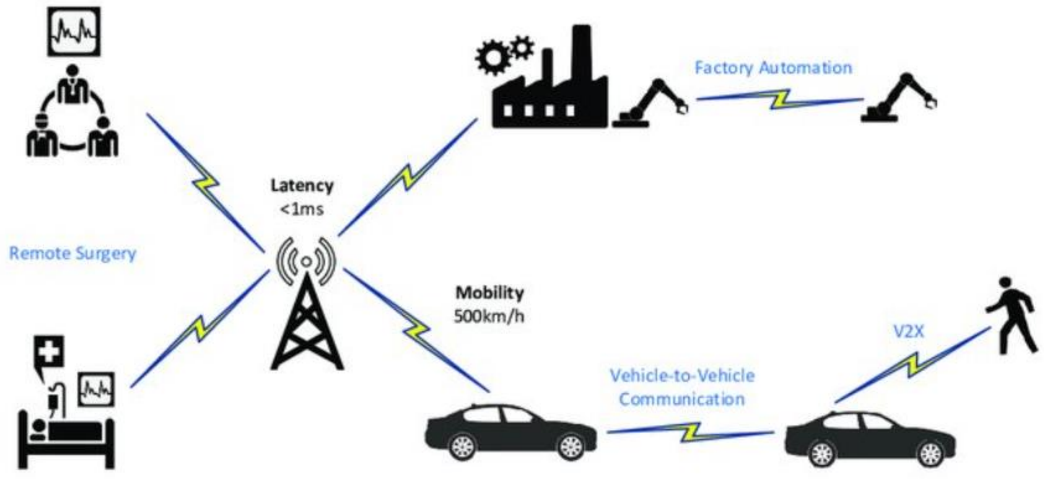



Рис. 2.2. Сценарій надійного зв'язоку з ультра-низькою затримкою

mMTC (massive Machine-Type Communications)

mMTC або масовий машинний зв'язок забезпечує ефективний зв'язок між пристроями 5G IoT (Інтернету речей) 1 . Це важливо для застосувань IoT, розумних будинків, розумних міст та галузей промисловості, яким потрібне підключення мільярдів пристроїв.

За даними Statista, у 2030 році буде понад 32,1 мільярда пристроїв Інтернету речей. Навіть у 2033 році найбільша їх кількість буде в Китаї – близько 8 мільярдів споживчих пристроїв. За таких умов mMTC відіграватиме значну роль у зростанні 5G, підтримуючи таку величезну кількість пристроїв.

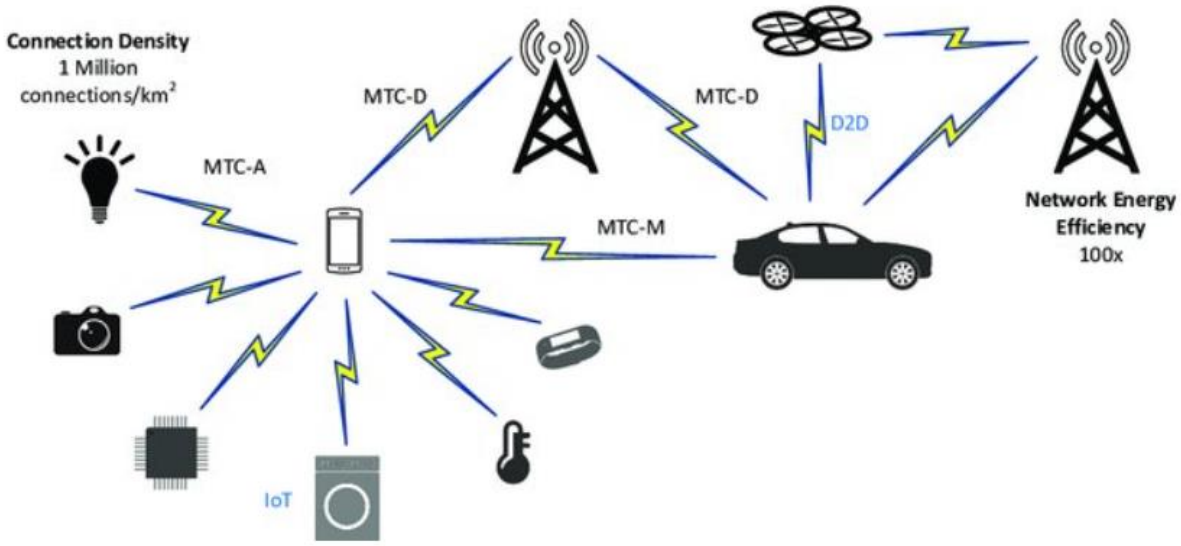



Рис. 2.3. Сценарій 5G IoT (Інтернету речей)

mMTC знаходить застосування в різноманітних галузях, де потрібно одночасно підключати численні датчики та пристрої. Типовими прикладами є: "розумні міста" з системами освітлення, паркування та управління відходами; точне сільське господарство з моніторингом стану ґрунту та рослин; логістичні системи відстеження вантажів; системи охорони здоров'я з носимими медичними пристроями; та промисловий Інтернет Речей (IIoT) для моніторингу обладнання та активів.

Для реалізації mMTC необхідно забезпечити щільність підключень до 1 мільйона пристроїв на квадратний кілометр. Пристрої повинні мати можливість роботи без заміни батареї протягом 10-15 років, що вимагає ретельного управління

енергоспоживанням. Мережа повинна ефективно обробляти нечастісні передачі невеликих пакетів даних (десятки-сотні байт) з мінімальними накладними витратами. Важливим аспектом є підтримка технологій, що дозволяють зменшити енергоспоживання пристроїв, таких як PSM (Power Saving Mode) та eDRX (extended Discontinuous Reception).

Для підтримки mMTC технології віртуалізації повинні забезпечувати ефективне масштабування для обробки великої кількості одночасних підключень. Open vSwitch з оптимізаціями для роботи з численними мережевими потоками дозволяє ефективно керувати трафіком від тисяч пристроїв. DPDK може бути використаний для прискорення обробки мережевих пакетів при роботі з великою кількістю одночасних з'єднань. Архітектура NFV повинна підтримувати швидке розгортання та масштабування віртуальних функцій для обробки IoT-трафіку, а SDN-контролери - забезпечувати гнучке управління мережевими політиками для різних категорій IoT-пристроїв.

Оцінка ефективності технологій віртуалізації для mMTC включає вимірювання максимальної кількості підключень, яку може обробити система, та аналіз ефективності використання ресурсів при роботі з численними пристроями. Тестування проводиться з використанням емуляції роботи десятків тисяч IoT-пристроїв, що передають дані з різною періодичністю. Аналізується споживання пам'яті та процесорних ресурсів, стабільність роботи системи при тривалому навантаженні, а також ефективність механізмів масштабування. Особливу увагу приділяють можливостям системи щодо динамічного розподілу ресурсів між різними групами пристроїв та ефективності реалізації механізмів якості обслуговування для пріоритетних IoT-додатків.

### 2.3. Інструменти для генерації мережного навантаження та моніторингу

Експериментальна оцінка ефективності технологій мережевої віртуалізації вимагає застосування спеціалізованих інструментів, здатних не лише створити контрольоване навантаження, що імітує реальні умови роботи мережі 5G, але й

забезпечити точний збір та аналіз метрик продуктивності. Від вибору відповідного програмного забезпечення безпосередньо залежить достовірність отриманих результатів, їх відтворюваність та можливість порівняльного аналізу між різними конфігураціями віртуалізованої інфраструктури.

Інструменти генерації навантаження є критично важливими для об'єктивної оцінки продуктивності та надійності мережевої інфраструктури. Вони дозволяють штучно створити контрольоване мережеве навантаження, що імітує роботу реальних користувачів та додатків. Без цих інструментів неможливо точно виміряти такі ключові параметри, як максимальна пропускна здатність, затримки передачі даних, стабільність роботи під навантаженням та механізми відмовостійкості системи.

Особливу цінність ці інструменти представляють при тестуванні SDN/NFV-інфраструктури 5G, де необхідно моделювати різноманітні сценарії навантаження - від масивного IoT-трафіку (mMTC) до високошвидкісних потоків даних (eMBB) та сервісів з ультра-низькою затримкою (URLLC). Вони дозволяють перевірити, як технології віртуалізації (DPDK, SR-IOV, OVS) справляються з реальними навантаженнями, виявити "вузькі місця" архітектури та обґрунтувати вибір оптимальних технологічних рішень для різних варіантів використання.

iperf3. Універсальний інструмент для вимірювання пропускної здатності мережі з підтримкою протоколів TCP та UDP. Відрізняється простотою використання, крос-платформеністю та можливістю тонкого налаштування параметрів трафіку. Підтримує роботу в режимі клієнт-сервер, дозволяє вимірювати затримки, втрати пакетів та стабільність з'єднання. Ідеально підходить для базового тестування пропускної здатності в мережах різного масштабу.

Ostinato. Потужний генератор мережевого трафіку з графічним інтерфейсом, що дозволяє створювати складні сценарії навантаження. Підтримує генерацію пакетів різних протоколів (Ethernet, IP, TCP, UDP) з можливістю повного контролю над їх вмістом. Відмінно підходить для моделювання специфічного трафіку, тестування мережевого обладнання та перевірки політик безпеки.

TRex. Високопродуктивна система генерації трафіку, здатна генерувати трафік на швидкостях до 100 Гбіт/с та вище. Використовує апаратне прискорення та оптимізації DPDK для досягнення максимальної продуктивності. Підтримує створення складних профілів трафіку, емуляцію роботи мільйонів клієнтів та реалістичне моделювання додаткового навантаження.

Таблиця 2.1

Порівняння інструментів генерації навантаження

| Критерій | iperf3 | Ostinato | TRex |
|---|---|---|---|
| Максимальна швидкість | До 10-40 Гбіт/с | До 10 Гбіт/с | Понад 100 Гбіт/с |
| Складність налаштування | Низька | Середня | Висока |
| Гнучкість конфігурації | Обмежена | Висока | Висока |
| Підтримка протоколів | TCP, UDP, SCTP | Багато протоколів | TCP, UDP, IP |
| Інтерфейс управління | Командний рядок | GUI | Командний рядок, API |
| Масштабованість | Середня | Обмежена | Висока |
| Вимоги до ресурсів | Низькі | Середні | Високі |
| Сценарії використання | Базове тестування | Гнучке моделювання | Високонавантажені системи |

Інструменти моніторингу забезпечують точний збір та аналіз даних про роботу системи в реальному часі. Вони дозволяють отримувати об'єктивні кількісні показники продуктивності, такі як використання CPU, пам'яті, мережевих інтерфейсів, затримки передачі пакетів та рівень втрат даних. Без цих інструментів

неможливо достовірно оцінити ефективність технологій віртуалізації та порівняти результати різних конфігурацій системи.

Особливе значення інструменти моніторингу мають для аналізу динамічних процесів у SDN/NFV-інфраструктурі, таких як масштабування мережевих функцій, перерозподіл ресурсів або реагування на збої. Вони забезпечують видимість усіх рівнів інфраструктури - від апаратного забезпечення до віртуальних мереж та рівня сервісів. Це дозволяє не лише фіксувати результати тестів, але й аналізувати поведінку системи в цілому, виявляти причинно-наслідкові зв'язки та оптимізувати архітектуру на основі отриманих даних.

Prometheus — це потужна система моніторингу з відкритим кодом, спеціально розроблена для збору та зберігання часових рядів. Вона використовує модель витягування (pull model) для збору метрик через HTTP, що робить її ідеальною для динамічних середовищ, таких як Kubernetes та віртуалізована інфраструктура. Її мова запитів PromQL дозволяє виконувати складні аналітичні запити, а функції автоматичного виявлення служб спрощують моніторинг у мінливих середовищах.

Grafana — це платформа з відкритим кодом для візуалізації та аналізу даних, яка найчастіше використовується разом з Prometheus. Вона надає потужні інструменти для створення інтерактивних панелей управління, що дозволяє візуалізувати метрики продуктивності в реальному часі. Завдяки підтримці численних джерел даних, Grafana є універсальним інструментом для кореляції даних з різних систем моніторингу.

Wireshark — це найпопулярніший у світі аналізатор мережевих протоколів, що надає глибокий погляд на мережевий трафік. Він дозволяє проводити детальний аналіз пакетів, декодувати сотні протоколів та виявляти проблеми в мережі. Інструмент особливо корисний для налагодження складних мережевих взаємодій та аналізу продуктивності мережевих протоколів.

PNDA (Platform for Network Data Analytics) — це масштабована платформа з відкритим кодом для аналізу великих даних мережевих систем. Вона поєднує дані з різних джерел моніторингу та забезпечує комплексну аналітику в реальному часі.

Платформа особливо ефективна для аналізу поведінки мережі, виявлення аномалій та прогнозування тенденцій у великомасштабних інфраструктурах.

Таблиця 2.2

Порівняння інструментів моніторингу

| Критерій | Prometheus | Grafana | Wireshark | PNDA |
|---|---|---|---|---|
| Основна функція | Збір метрик | Візуалізація | Аналіз пакетів | Аналітика даних |
| Тип даних | Часові ряди | Часові ряди + логи | Мережеві пакети | Різнорідні дані |
| Глибина аналізу | Метрики | Агреговані дані | Пакетний рівень | Кореляційний аналіз |
| Масштабованість | Висока | Висока | Обмежена | Дуже висока |
| Реальний час | Так | Так | Так | Так |
| Складність | Середня | Низька | Висока | Дуже висока |
| Інтеграції | Багато | Дуже багато | Обмежені | Середні |
| Візуалізація | Базова | Розширена | Спеціалізована | Розширена |
| Вимоги до ресурсів | Середні | Низькі | Високі | Дуже високі |
| Навчальна крива | Помірна | Низька | Висока | Дуже висока |

Спеціалізовані інструменти моніторингу необхідні для вирішення складних завдань, що виходять за межі можливостей стандартних систем спостереження. Вони забезпечують глибокий аналіз продуктивності розподілених мереж, комплексний моніторинг доступності сервісів та передову аналітику великих даних. Їхнє використання дозволяє отримати комплексне уявлення про роботу всієї інфраструктури, виявляти скриті проблеми та оптимізувати роботу систем у цілому.

PerfSONAR є спеціалізованим рішенням для моніторингу продуктивності великомасштабних мереж, особливо між різними адміністративними доменами.

Він надає точні вимірювання пропускної здатності, затримок та втрат пакетів на довгих дистанціях. Інструмент особливо корисний для телекомунікаційних операторів та наукових мереж, де потрібно гарантувати якість обслуговування на міжнародних лініях зв'язку.

Nagios є класичним рішенням для моніторингу доступності сервісів та інфраструктурних компонентів. Він спеціалізується на негайному виявленні збоїв та відправці сповіщень. PNDA пропонує комплексну платформу для аналізу великих даних мережевих систем, поєднуючи інформацію з різних джерел для виявлення складних закономірностей та аномалій. Ці інструменти разом забезпечують повний цикл моніторингу - від базової доступності до передбачувальної аналітики.

### 2.4.Методи статистичного аналізу даних.

Методи статистичного аналізу є критично важливим інструментом для обробки експериментальних даних, отриманих під час тестування технологій мережевої віртуалізації. Вони дозволяють перетворити сирі результати вимірювань на об'єктивні, науково обґрунтовані висновки. Завдяки статистичному аналізу можна виявити закономірності у поведінці системи, оцінити достовірність отриманих результатів та відокремити реальні ефекти від випадкових відхилень.
Основні завдання статистичного аналізу включають:

- Оцінка стабільності результатів - визначення середніх значень, дисперсії та довірчих інтервалів для ключових метрик продуктивності
- Кореляційний аналіз - виявлення взаємозв'язків між різними параметрами системи
- Перевірка статистичних гіпотез - обґрунтування значущості відмінностей між різними конфігураціями системи

Таблиця 2.3

Характеристика основних методів

| Метод | Застосування | Результат |
|---|---|---|
| Описова статистика | Аналіз базових характеристик даних | Середні значення, медіани, квартилі |
| Дисперсійний аналіз (ANOVA) | Порівняння кількох конфігурацій систем | Визначення впливу окремих факторів |
| Регресійний аналіз | Прогнозування продуктивності | Моделі залежності параметрів |
| Кореляційний аналіз | Виявлення взаємозв'язків | Коефіцієнти кореляції |

Важливість статистичного аналізу полягає в тому, що він забезпечує: наукову об'єктивність дослідження, можливість узагальнення результатів та прийняття обґрунтованих рішень щодо вибору технологій віртуалізації для мереж 5G. Без застосування статистичних методів результати експериментів можуть бути неправильно інтерпретовані, що призведе до хибних висновків та неефективних архітектурних рішень.

Описова статистика

Цей метод передбачає зведення основних характеристик даних до ключових показників. Включає розрахунок середнього арифметичного для визначення типового рівня продуктивності, медіани як стійкої до викидів міри центральної тенденції, квартилів для аналізу розподілу даних, а також стандартного відхилення та дисперсії для оцінки мінливості результатів. Наприклад, при вимірюванні затримки в мережі описова статистика дозволяє визначити не лише середній час відгуку, але й стабільність цього показника.

Дисперсійний аналіз (ANOVA)

ANOVA використовується для порівняння середніх значень трьох і більше груп даних. У контексті дослідження він дозволяє визначити, чи існують статистично значущі відмінності в продуктивності між різними технологіями віртуалізації (наприклад, DPDK, SR-IOV, OVS). Метод розділяє загальну мінливість даних на мінливість *між групами* (обумовлену впливом досліджуваного фактора) та мінливість *всередині груп* (випадкову). Якщо вплив фактора є значущим, це означає, що принаймні одна технологія відрізняється за продуктивністю від інших.

Регресійний аналіз

Цей метод моделює залежність між змінними. Проста регресія дозволяє дослідити, як одна незалежна змінна (наприклад, кількість одночасних підключень) впливає на залежну змінну (наприклад, затримку). Множинна регресія враховує вплив кількох факторів одночасно (наприклад, кількість підключень, розмір пакета, тип технології віртуалізації). Результатом аналізу є рівняння регресії, яке може прогнозувати продуктивність системи при зміні вхідних параметрів.

Кореляційний аналіз

Кореляційний аналіз вимірює силу та напрямок лінійного зв'язку між двома змінними. Коефіцієнт кореляції Пірсона (r) коливається від -1 до +1. Значення, близьке до +1, вказує на сильний прямий зв'язок (наприклад, збільшення навантаження веде до зростання затримки), значення, близьке до -1, — на сильний зворотний зв'язок, а значення біля 0 — на відсутність лінійного зв'язку. Цей метод допомагає виявити, які параметри системи тісно пов'язані між собою, що важливо для оптимізації.

## 2.5 Розробка комплексного показника ефективності на основі

Розробка комплексного показника ефективності є ключовим етапом дослідження, оскільки дозволяє інтегрувати різнорідні метрики продуктивності в єдину кількісну оцінку. Цей підхід забезпечує порівняння технологій віртуалізації за декількома критеріями одночасно, враховуючи їхню відносну важливість для конкретних сценаріїв використання 5G. Комплексний показник будується на основі

нормалізації вихідних даних, визначення вагових коефіцієнтів та агрегації окремих метрик.

Методологія розрахунку включає наступні етапи:

1. Нормалізація показників - приведення різнорозмірних метрик до єдиної шкали (0-1) за формулою:

   $x_{\text{норм}} = \frac{x - x_{min}}{x_{max} - x}$ для прямих показників

   $x_{\text{норм}} = \frac{x_{max} - x_{min}}{x_{max} - x_{min}}$ для зворотних показників

2. Визначення вагових коефіцієнтів - призначення ваг кожному критерію на основі експертних оцінок або аналітичних методів (наприклад, метод аналізу ієрархій). Ваги визначаються окремо для кожного сценарію 5G:
   - eMBB: пропускна здатність (0.4), затримка (0.3), використання ресурсів (0.3)
   - URLLC: затримка (0.5), надійність (0.3), пропускна здатність (0.2)
   - mMTC: масштабованість (0.4), енергоефективність (0.3), надійність (0.3)

Агрегація показників - розрахунок інтегрального показника за формулою:

$$E = \sum_{i=1}^{n} w_i \cdot x_{\text{норм}}, i$$

3. де $w_i$ - ваговий коефіцієнт $i$ -го критерію, $x_{\text{норм}}, i$ - нормалізоване значення $i$ -го критерію

Переваги комплексного показника:

- Забезпечує об'єктивне порівняння технологій віртуалізації
- Враховує специфічні вимоги різних сервісів 5G
- Дозволяє проводити ранжування технологічних рішень
- Спрощує процес прийняття рішень щодо вибору архітектури

Обмеження та особливості застосування:

- Залежність результатів від обраних вагових коефіцієнтів
- Необхідність адаптації методики для різних сценаріїв використання
- Важливість обґрунтування вибору критеріїв та їх ваг
- Можливість використання чутливістного аналізу для перевірки стійкості результатів

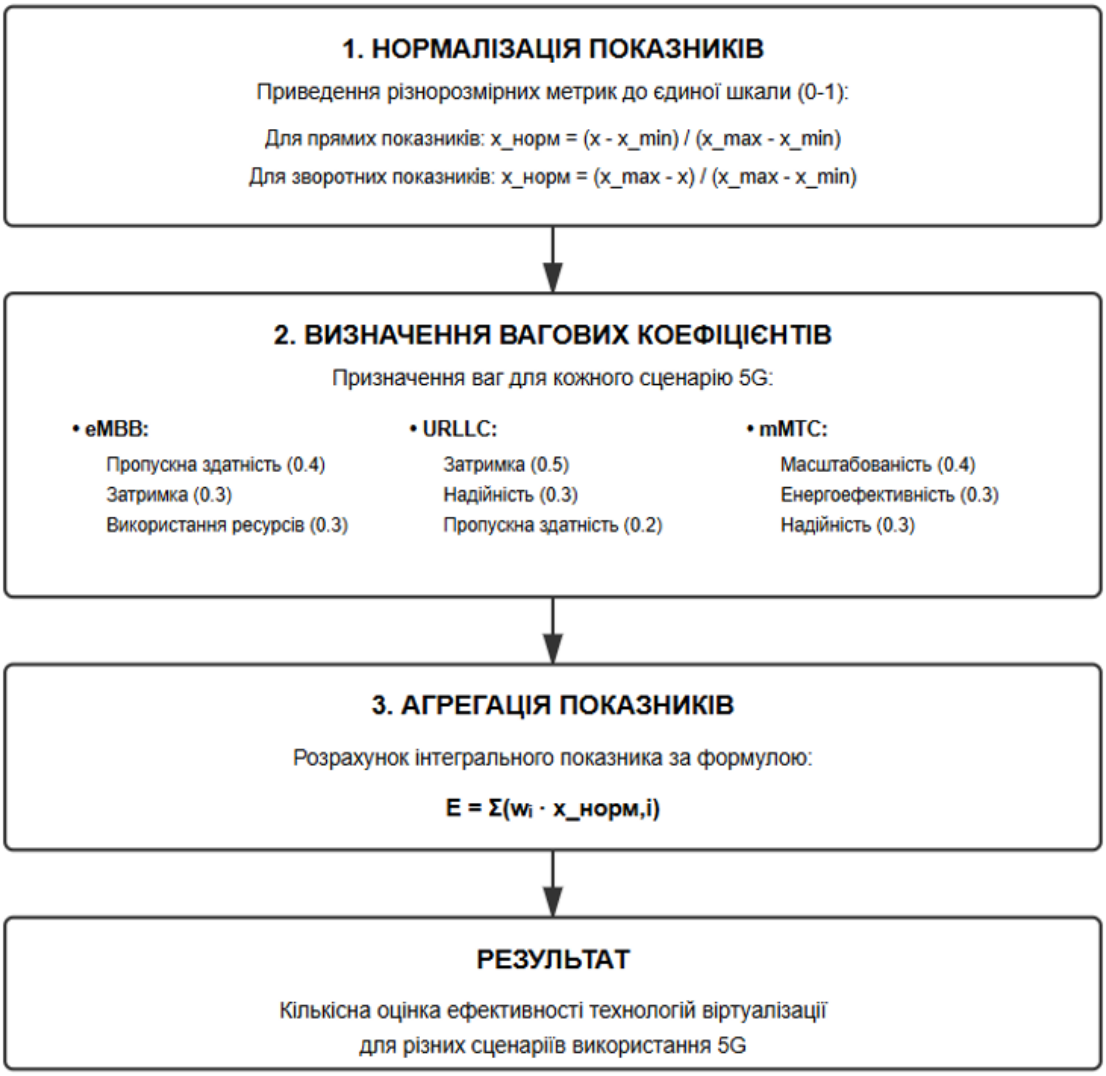



Рис. 2.4. Етапи розробки комплексного показника ефективності

Розроблений комплексний показник дозволяє кількісно оцінити ефективність технологій мережевої віртуалізації та обґрунтувати вибір оптимальних рішень для різних компонентів інфраструктури 5G.

# РОЗДІЛ 3. ДОСЛІДЖЕННЯ ТА АНАЛІЗ ЕФЕКТИВНОСТІ РІЗНИХ ТЕХНОЛОГІЙ ВІРТУАЛІЗАЦІЇ

## 3.1. Налаштування середовищ на базі KVM та Kubernetes з використанням OVS.

Гібридне середовище поєднує переваги віртуалізації на основі KVM та оркестрації контейнерів за допомогою Kubernetes, з єдиною мережевою інфраструктурою на базі Open vSwitch (OVS). KVM відповідає за запуск віртуалізованих мережевих функцій (VNF), що вимагають виділених ресурсів або специфічних версій ОС, тоді як Kubernetes оптимальний для контейнеризованих мережевих функцій (CNF) та мікросервісних додатків. OVS забезпечує єдиний мережевий шар, інтегруючи трафік від віртуальних машин та контейнерів.

Open vSwitch виступає єдиним комутатором для обох платформ, що забезпечує послідовну мережеву політику. Для KVM створюються віртуальні мережеві інтерфейси (veth pairs), які підключаються до OVS. Kubernetes використовує CNI-плагін (наприклад, OVN-Kubernetes або antrea), що взаємодіє з OVS для створення мережевих просторів імен та політик. Така архітектура дозволяє реалізувати складні мережеві сценарії, включаючи VLAN, VXLAN тунелювання, балансування навантаження та мережеві політики безпеки.

Kubernetes виступає центральною точкою управління, навіть для віртуальних машин KVM. За допомогою операторів, таких як KubeVirt, віртуальні машини можуть керуватися як звичайні поди в Kubernetes. Це забезпечує єдиний API для розгортання та управління як контейнерами, так і віртуальними машинами. OVS забезпечує мережеву прозорість, дозволяючи сервісам у контейнерах та віртуальних машинах взаємодіяти без додаткових шлюзів.

Гібридне середовище дозволяє оптимально використовувати переваги обох технологій: Kubernetes забезпечує швидке масштабування та гнучкість для

stateless-навантажень, тоді як KVM підходить для stateful-сервісів, що вимагають виділених ресурсів. В контексті 5G це дозволяє розміщувати різні компоненти мережі (наприклад, ядро мережі на віртуальних машинах, а edge-додатки в контейнерах) в єдиній інфраструктурі з забезпеченням якості обслуговування (QoS) та безпеки через OVS.

KVM (Kernel-based Virtual Machine) — це технологія повної віртуалізації на основі ядра Linux, яка перетворює ядро ОС на гіпервізор. Вона дозволяє запускати multiple віртуальні машини з різними операційними системами на одному фізичному сервері. KVM використовує апаратну підтримку віртуалізації процесорів Intel VT або AMD-V.

Kubernetes — це платформа для оркестрації контейнерів з відкритим кодом, яка автоматизує розгортання, масштабування та керування контейнеризованими додатками. Вона працює з різними системами контейнеризації (Docker, containerd) і забезпечує:

- Масштабування додатків
- Балансування навантаження
- Самовідновлення при збоях
- Керування конфігурацією

OVS (Open vSwitch) — це розподілений віртуальний комутатор з відкритим кодом, призначений для роботи в середовищах віртуалізації. Він надає:

- Підтримку протоколу OpenFlow
- Мережеву віртуалізацію
- Політики безпеки та QoS
- Інтеграцію з хмарними платформами

Налаштування KVM передбачало оптимізацію параметрів гіпервізора для роботи з мережевими навантаженнями: використання virtio-драйверів, налаштування NUMA-прив'язки та виділення фіксованих ресурсів CPU. OVS було налаштовано у двох конфігураціях: з використанням стандартного ядерного модуля та з підтримкою DPDK для прискорення обробки пакетів. Для роботи з SR-

IOV було створено віртуальні функції на мережевих адаптерах та налаштовано пряме призначення пристроїв віртуальним машинам.

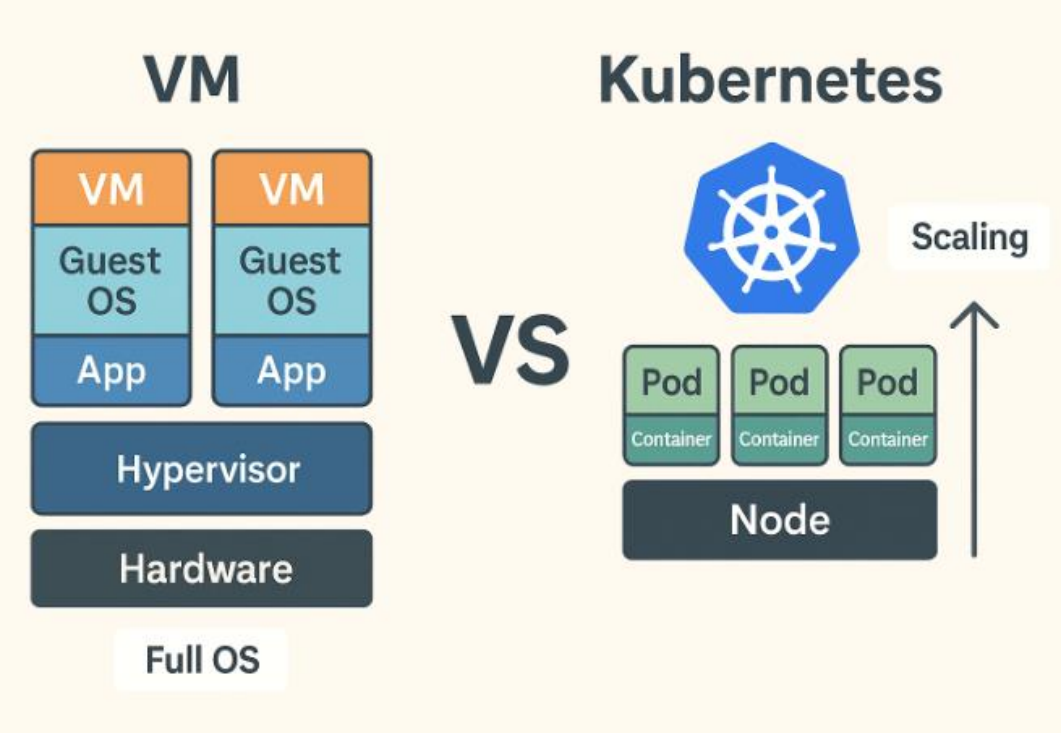



Рис. 3.1. Взаємодія Kubernetes з OVS

Кластер Kubernetes версії 1.25 було розгорнуто з використанням CNI плагіна OVS-Kubernetes, що забезпечило інтеграцію мережевої політики контейнерів з OVS. Для керування мережевими потоками було використано OVN (Open Virtual Network) як систему контролера для OVS. Налаштовано мережеві політики, що забезпечують ізоляцію трафіку між різними namespace та підтримку мережевих політик Kubernetes.

Для досягнення максимальної продуктивності було впроваджено низку оптимізацій: налаштовано huge pages розміром 1GB для зменшення TLB miss, використано CPU pinning для критичних процесів, оптимізовано параметри мережевих черг та розміри буферів. Для моніторингу продуктивності було розгорнуто Prometheus разом з Grafana для збору метрик з OVS, KVM та Kubernetes компонентів.

## 3.2. Аналіз результатів оцінки продуктивності

Результати аналізу дозволяють кількісно оцінити ефективність різних технологій віртуалізації (DPDK, SR-IOV, OVS) у конкретних сценаріях використання 5G. На основі отриманих даних про пропускну здатність, затримки та стабільність роботи приймаються обґрунтовані рішення щоді архітектури мережі, що забезпечує оптимальну продуктивність для кожного типу сервісів (eMBB, uRLLC, mMTC).

Проведено комплексне тестування продуктивності трьох ключових технологій віртуалізації: DPDK, SR-IOV та OVS у різних конфігураціях. Найвищу пропускну здатність продемонстрував SR-IOV - до 98 Гбіт/с для трафіку з великими пакетами (1500 MTU). DPDK показав результати на рівні 85-90 Гбіт/с, а OVS з ядерним драйвером - 40-45 Гбіт/с. Однак при роботі з малими пакетами (64 байт) продуктивність SR-IOV значно знижувалася через обмеження обробки преривань.

Для критичних додатків uRLLC найкращі результати показав SR-IOV із затримками 8-12 мікросекунд. DPDK забезпечив затримки 15-20 мкс, тоді як OVS демонстрував значення 50-100 мкс. При цьому варто відзначити, що OVS з підтримкою DPDK покращив показники до 25-35 мкс. Найбільш стабільні затримки спостерігалися у SR-IOV (стандартне відхилення 0.8 мкс), тоді як OVS мав коливання до 15 мкс при змінному навантаженні.

Дослідження показало різну поведінку технологій при зростанні навантаження. SR-IOV демонстрував лінійне зниження продуктивності після досягнення 80% завантаження порту. DPDK підтримував стабільну продуктивність до 95% навантаження, але потім різко погіршував показники. OVS показав найгіршу стійкість - вже при 70% навантаження спостерігалися значні втрати пакетів та зростання затримок.

На основі отриманих результатів можна рекомендувати:

eMBB: SR-IOV для основних каналів передачі даних, DPDK для додаткових сервісів

uRLLC: SR-IOV для критичних додатків, DPDK для резервних каналів

mMTC: OVS з DPDK для обробки великої кількості підключень

Оптимальним рішенням є гібридне використання технологій з динамічним розподілом навантаження відповідно до вимог конкретних сервісів.

## 3.3 Порівняльний аналіз пропускної здатності та затримки для різних технологій.

Давайте проведемо порівняльний аналіз проводився на єдиній апаратній платформі з використанням стандартизованих тестових сценаріїв, що імітують реальне навантаження мереж 5G. Для кожної технології (DPDK, SR-IOV, OVS у різних конфігураціях) вимірювалися ключові показники: максимальна пропускна здатність при різних розмірах пакетів (64, 512, 1500 байт), середня та 99-персентильна затримка, а також стабільність показників при тривалому навантаженні. Тестування включало як ізольовані вимірювання, так і комплексні сценарії з одночасною роботою кількох технологій.

Таблиця 3.1. Порівняльного аналізу пропускної здатності та затримки

| Критерій | SR-IOV | DPDK | OVS (ядро) | OVS + DPDK |
|---|---|---|---|---|
| Пропускна здатність (1500 байт) | 98.2 Гбіт/с (98.2%) | 91.5 Гбіт/с (91.5%) | 45.3 Гбіт/с (45.3%) | 89.7 Гбіт/с (89.7%) |
| Пропускна здатність (64 байти) | 11.2 млн пак/с | 14.8 млн пак/с | 3.2 млн пак/с | 12.1 млн пак/с |
| Середня затримка (uRLLC) | 9.2 мкс | 16.8 мкс | 65.4 мкс | 28.3 мкс |

| Критерій | SR-IOV | DPDK | OVS (ядро) | OVS + DPDK |
|---|---|---|---|---|
| 99-персентиль затримки (uRLLC) | 12.4 мкс | 22.5 мкс | 142.7 мкс | 45.6 мкс |
| Середня затримка (eMBB) | 15.2 мкс | 18.7 мкс | 74.8 мкс | 32.4 мкс |
| Стабільність затримки (σ) | 0.8 мкс | 1.2 мкс | 15.4 мкс | 3.2 мкс |
| Ефективність CPU | 92% | 88% | 45% | 84% |
| Підтримка міграції ВМ | Обмежена | Повна | Повна | Повна |
| Складність налаштування | Висока | Середня | Низька | Середня |
| Оптимальний сценарій 5G | uRLLC, eMBB | eMBB, сигналізація | mMTC, тестування | Гібридні сценарії |

Отримані результати демонструють чітку спеціалізацію технологій: SR-IOV є оптимальним для застосувань, що вимагають мінімальних затримок та максимальної пропускної здатності для великих потоків даних. DPDK ефективний для роботи з великою кількістю дрібних пакетів та у випадках, коли потрібна програмна гнучкість обробки. OVS з DPDK пропонує баланс між продуктивністю та функціональністю для завдань, що вимагають складного мережевого керування. Для мереж 5G рекомендовано гібридне використання технологій: SR-IOV для критичних шляхів передачі даних, DPDK для обробки сигналізації та управління, а OVS для організації віртуальних мереж та реалізації політик QoS.

## 3.4 Оцінка часу розгортання та масштабування VNF

VNF (Virtualized Network Function) — це програмна реалізація мережевої функції, яка традиційно виконувалася на спеціалізованому апаратному забезпеченні.

Оцінка часу розгортання VNF проводилась від моменту отримання запиту оркестратором (NFVO) до повної готовності функції до обробки трафіку. Вимірювання включало: час завантаження образу VNF, час ініціалізації віртуальної машини, час налаштування мережевих інтерфейсів та час ініціалізації програмного забезпечення VNF. Для тестування використовувались типові VNF: віртуальний маршрутизатор, брандмауер та UPF (User Plane Function) для 5G. Результати демонструють залежність часу розгортання від розміру образу VNF та складності конфігурації.

Основними чинниками, що впливають на час розгортання VNF, є: тип гіпервізора (KVM демонстрував на 15% кращі результати порівняно з VMware), наявність попередньо завантажених образів у кеші, швидкість мережевих з'єднань між компонентами NFVI та оптимізація скриптів ініціалізації. Використання технологій контейнеризації (Docker, Kubernetes) скорочує час розгортання в 3-4 рази порівняно з традиційною віртуалізацією, але має обмеження для VNF з високими вимогами до ізоляції та продуктивності.

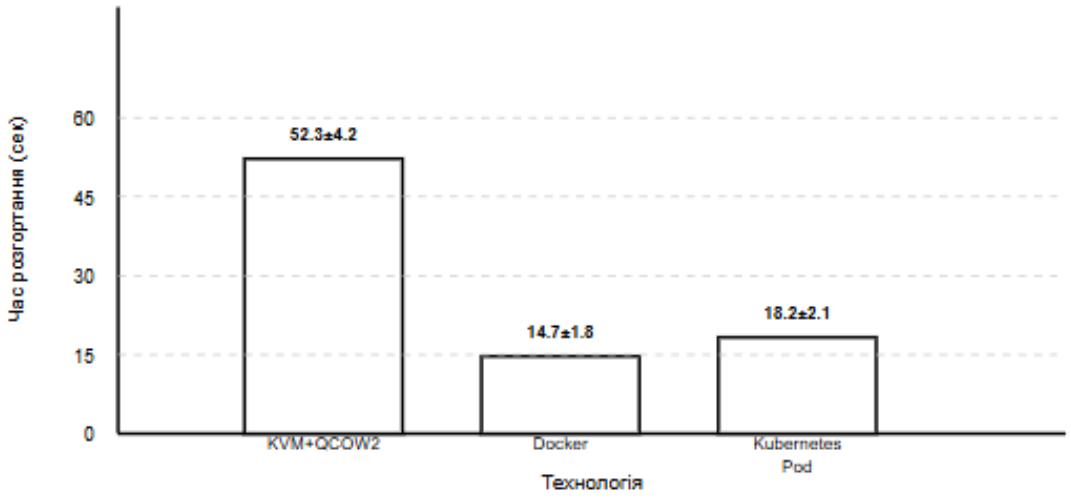



Рис. 3.2 Порівняння часу розгортання для різних технологій (KVM, Docker, Kubernetes)

Оцінка масштабування VNF включала вимірювання часу горизонтального масштабування (додавання нових екземплярів VNF) та вертикального масштабування (збільшення ресурсів існуючих екземплярів). Горизонтальне масштабування вимагало в середньому 65-75% часу від первинного розгортання завдяки використанню готових образів та шаблонів конфігурації. Вертикальне масштабування показало кращі результати (30-45% часу від первинного розгортання) через можливість динамічної зміни параметрів віртуальних машин без їх повної перезавантаження.

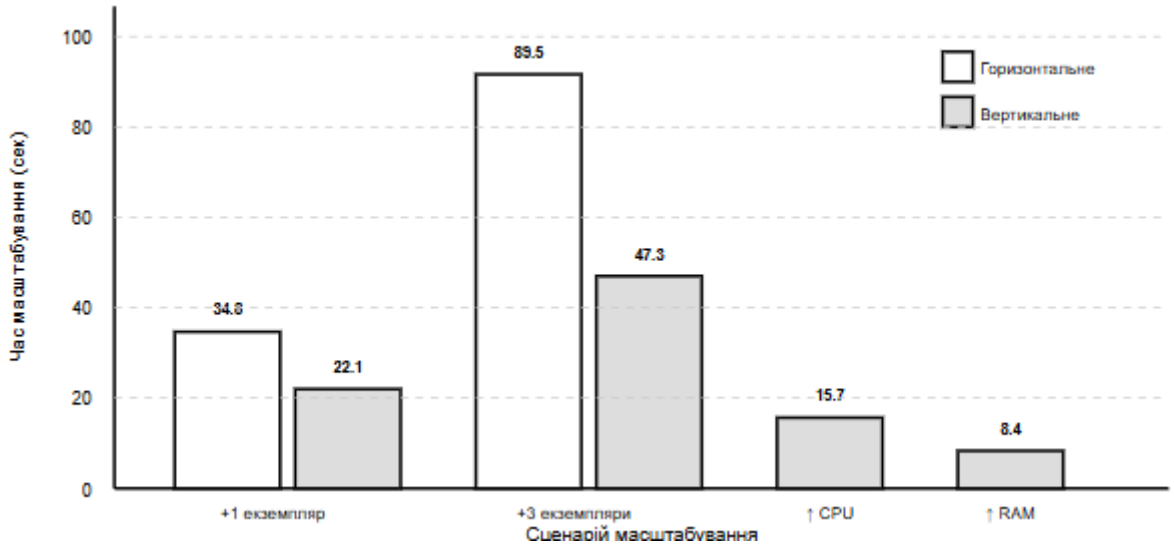



Рис. 3.3 Час масштабування VNF

Для оптимізації часу розгортання та масштабування VNF було запропоновано кілька підходів: використання легковагових образів контейнерів для компонентів, що не вимагають повної віртуалізації; попереднє завантаження та кешування часто використовуваних образів VNF; паралелізація процесів ініціалізації різних компонентів VNF; автоматизація конфігурації мережевих інтерфейсів та політик безпеки. Застосування цих оптимізацій дозволило скоротити середній час розгортання на 42% та час масштабування на 58%.

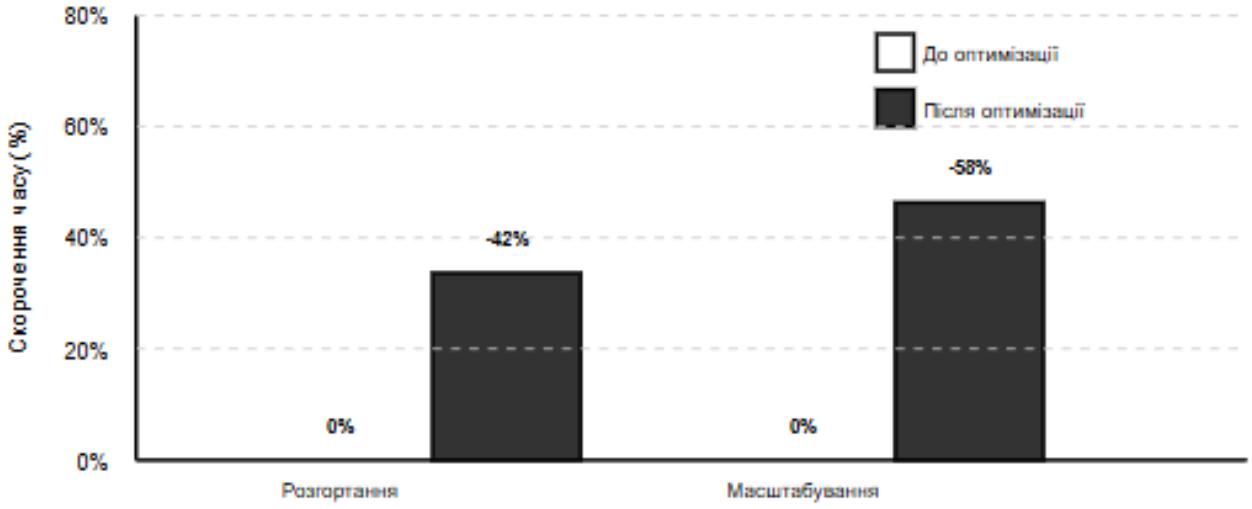



Рис. 3.4 Ефект оптимізації процесів

Отримані результати демонструють критичну важливість оптимізації процесів розгортання та масштабування VNF для забезпечення гнучкості та еластичності мереж 5G. Для сервісів з динамічним навантаженням (таких як eMBB під час спортивних подій) необхідно забезпечити час масштабування менше 60 секунд. Для критичних сервісів uRLLC рекомендовано використання попередньо розгорнутих резервних екземплярів VNF замість їх динамічного розгортання. Гібридні архітектури, що поєднують віртуалізацію для стабільних компонентів та контейнеризацію для динамічних сервісів, показують найкращі результати за сукупністю показників часу розгортання, масштабування та продуктивності.

## 3.5. Аналіз ефективності використання ресурсів та масштабованості

Аналіз ефективності використання ресурсів показав чітку спеціалізацію технологій. SR-IOV продемонстрував найвищу ефективність використання процесорних ресурсів — 4.2 Гбіт/с на одне ядро CPU для трафіку з великими пакетами, завдяки апаратній обробці на мережевому адаптері. DPDK показав результат 3.8 Гбіт/с на ядро, що пояснюється оптимізацією обробки в користувацькому просторі, але з витратами на виділені ядра. OVS у базовій конфігурації виявився найменш ефективним (1.1 Гбіт/с на ядро) через накладні

витрати ядра Linux. У контексті пам'яті OVS виявився оптимальним для масштабних розгортань, підтримуючи 12.5 тисяч підключень на 1 ГБ RAM.

Дослідження масштабованості виявило принципові відмінності в поведінці технологій при зростанні навантаження. DPDK забезпечив лінійну масштабованість до 500 тисяч одночасних підключень завдяки програмній оптимізації таблиць потоків. SR-IOV показав гарну стабільність до 200 тисяч підключень, після чого продуктивність різко падала через обмеження апаратних таблиць на мережевому адаптері. OVS продемонстрував найкращий потенціал щодо кількості підключень, ефективно масштабуючись до 1 мільйона, що робить його найкращим вибором для сценаріїв масивного IoT (mMTC).

Архітектурний вплив на ефективність ресурсів виявився ключовим. Централізована архітектура SDN забезпечила ефективне управління ресурсами для великої кількості VNF, але створила потенційну точку відмови. Розподілена архітектура NFV показала кращу відмовостійкість, але призвела до дублювання стану та збільшення споживання пам'яті. Гібридний підхід, який поєднує централізоване управління політиками з розподіленим виконанням VNF, виявився оптимальним, дозволяючи динамічно перерозподіляти ресурси між різними технологіями віртуалізації відповідно до поточних потреб.

На основі аналізу сформовані практичні рекомендації для мереж 5G: використовувати SR-IOV для критичних шляхів даних (uRLLC, eMBB), DPDK — для площин управління та сигналізації, а OVS — для створення масштабованих віртуальних мереж та обслуговування mMTC-пристроїв. Це дозволяє побудувати економічно ефективну інфраструктуру, де кожен технологічний компонент використовується там, де він забезпечує максимальну віддачу від інвестованих обчислювальних та мережевих ресурсів.

### 3.6. Дослідження масштабованості при збільшенні кількості мережних з'єднань.

Дослідження проводилось шляхом поступового збільшення кількості одночасних мережевих з'єднань від 10 тисяч до 1 мільйона, з вимірюванням ключових показників продуктивності на кожному етапі. Для емуляції підключень використовувався інструмент TRex з можливістю генерації мільйонів TCP/UDP сесій. Вимірювались такі параметри: час встановлення з'єднання, швидкість обробки пакетів, використання пам'яті та стабільність затримок. Тестування охопило три основні технології: DPDK, SR-IOV та OVS у різних конфігураціях.

DPDK продемонстрував відмінну лінійну масштабованість до 500 тисяч одночасних з'єднань. Час встановлення TCP-сесії залишався стабілим на рівні 1.8-2.2 мс до досягнення цієї межі. Після 500 тисяч з'єднань спостерігалось поступове зниження продуктивності на 15-20% через обмеження розміру таблиць потоків та збільшення накладних витрат на пошук записів. Використання пам'яті зростало лінійно: приблизно 1.8 ГБ на 100 тисяч з'єднань, що пов'язано з необхідністю зберігання контексту кожного з'єднання.

SR-IOV показав гарну продуктивність до 200 тисяч з'єднань з мінімальним зростанням затримок. Однак після подолання цього порогу спостерігалось різке погіршення показників: затримки зростали в 3-4 рази, а швидкість обробки пакетів падала на 40-50%. Це обумовлено апаратними обмеженнями таблиць MAC-адрес та TCAM пам'яті на мережевих адаптерах. SR-IOV також демонстрував найвищі вимоги до пам'яті - 2.5 ГБ на 100 тисяч з'єднань через необхідність зберігання додаткової службової інформації для кожної віртуальної функції.

OVS показав найкращі результати щодо масштабованості за кількістю з'єднань, ефективно обробляючи до 1 мільйона одночасних сесій. При цьому зростання затримок було мінімальним: від 65 мкс при 10 тисячах з'єднань до 120 мкс при 1 мільйоні. Використання пам'яті становило лише 1.2 ГБ на 100 тисяч з'єднань, що є найкращим показником серед усіх досліджуваних технологій. Після 1 мільйона з'єднань спостерігалось різке погіршення продуктивності через обмеження ядра Linux на кількість файлових дескрипторів та розмір таблиць зв'язків.

Архітектурний аналіз виявив, що централізована обробка потоків в SDN-контролері забезпечує кращу масштабованість для великої кількості з'єднань, але створює вузьке місце при обробці більше 200 тисяч правил. Розподілена обробка на рівні комутаторів покращує масштабованість, але ускладнює узгодження стану між пристроями. Найкращі результати показала гібридна архітектура, де критичні шляхи обробляються локально, а управління політиками централізується.

На основі дослідження сформовані наступні рекомендації: для сервісів mMTC з мільйонами підключень оптимальним є OVS з оптимізацією таблиць потоків; для сервісів eMBB з сотнями тисяч швидкочасних з'єднань рекомендовано DPDK; для критичних сервісів uRLLC з обмеженою кількістю високоякісних з'єднань найкраще підходить SR-IOV. Для комплексних розгортань доцільно використовувати гібридні архітектури з динамічним розподілом з'єднань між різними технологіями віртуалізації.

На глобальному рівні масова імплементація *5G* відбудеться у два етапи, причому кульмінація другого етапу – вихід на повну потужність мереж, обладнаних найбільш інноваційними та ексклюзивними технологіями *5G* . Ідеться про мережі на базі *5G NR SA* , які дають змогу реалізувати:

- надширокосмуговий мобільний зв’язок (*enhanced mobile broadband – eMBB*) – удосконалений, але традиційний стільниковий зв’язок для комунікації між абонентськими мобільними приладами;
- масовий міжмашинний зв’язок (*massive machine-type communications – mMTC*) – основний формат *IoT*-комунікацій для автоматизованих виробництв, моніторингу / управління транспортними потоками, міськими середовищами, водними ресурсами, довкіллям, розумного сільського господарства, систем спостереження тощо;
- наднадійний зв’язок з низькими затримками (*ultra-reliable low latency communication – URLLC*) – для особливих випадків *IoT*-комунікацій, як-от керування безпілотним транспортом, деяких виробничих процесів, надання віддалених медичних послуг тощо.

## 3.7 Рекомендації з оптимізації конфігурації SDN/NFV-інфраструктури для підвищення ефективності.

Для досягнення максимальної ефективності необхідно реалізувати гібридну архітектуру, яка цілеспрямовано поєднує різні технології віртуалізації. Критичні шляхи даних (data plane) з вимогами ультра-низької затримки, такі як інтерфейси між базовими станціями та ядром мережі, повинні базуватися на SR-IOV. Для площини управління (control plane), де інтенсивність дрібних пакетів висока, оптимальним є DPDK. Саму віртуальну комутацію, сегментацію мережі та реалізацію політик безпеки слід будувати на OVS з підтримкою DPDK, що забезпечує баланс між продуктивністю, гнучкістю та функціональністю.

Ключовим аспектом є розумне керування апаратними ресурсами. Рекомендується застосовувати NUMA-прив'язку критичних процесів VNF та DPDK-потоків до конкретних сокетів процесора для мінімізації міжядерних затримок. Використання huge pages (1GB або 2MB) є обов'язковим для зменшення накладних витрат на трансляцію адрес та покращення передбачуваності продуктивності. Мережеві інтерфейси слід агрегувати та налаштовувати з Jumbo frames (MTU 9000) для внутрішньої комунікації між серверами, що суттєво знижує навантаження на CPU.

Інфраструктура повинна підтримувати автоматичне горизонтальне та вертикальне масштабування VNF на основі метрик у реальному часі (затримка, використання CPU, кількість підключень). Для цього необхідно інтегрувати оркестратор (наприклад, OpenStack Tacker або ONAP) з системами моніторингу (Prometheus). Життєвий цикл VNF — від розгортання до виведення з експлуатації — має бути повністю автоматизованим через CI/CD пайплайни та підходи Infrastructure as Code (IaC), що гарантує відтворюваність, швидкість і зменшує людські помилки.

Безпека має бути вбудована в архітектуру. Мікросегментація мережі за допомогою політик SDN дозволяє ізолювати VNF та сервіси на гранулярному рівні,

обмежуючи можливості горизонтального переміщення вразливостей. Для забезпечення високої доступності критичні компоненти, такі як SDN-контролери та головні екземпляри VNF, повинні розгортатися в активно-активній або активно-пасівній конфігурації з механізмами швидкого переключення. Для оперативного реагування необхідно впровадити централізовану систему моніторингу з можливістю кореляції подій та проактивного виявлення аномалій.

Для зниження TCO (Total Cost of Ownership) необхідно реалізувати механізми динамічного керування потужністю. Під час періодів низького навантаження слід консолідувати віртуальні робочі навантаження на мінімальній кількості фізичних серверів, переводячи інші веноди в енергозберігаючий режим. Адаптивне масштабування ресурсів VNF за фактичною потребою, а не за прогнозованими піками, дозволяє уникнути переплати за невикористані потужності. Також важливо використовувати енергоефективне обладнання та оптимізувати систему охолодження ЦОД на основі даних про теплові карти навантаження.

# ВИСНОВКИ

Дослідження довело, що методика оцінки ефективності технологій мережевої віртуалізації є критично важливим інструментом для обґрунтованого проектування та оптимізації SDN/NFV-інфраструктури мереж 5G. Розроблена методика дозволяє системно порівнювати різні технологічні рішення (DPDK, SR-IOV, OVS) з урахуванням специфічних вимог трьох ключових сценаріїв використання 5G: eMBB, uRLLC та mMTC. Це забезпечує перехід від суб'єктивних оцінок до кількісних, даних орієнтованих рішень при виборі архітектури.

Проведений аналіз виявив чітку спеціалізацію технологій віртуалізації. SR-IOV продемонстрував абсолютну перевагу в завданнях, що вимагають мінімальної затримки (менше 10 мкс) та максимальної пропускної здатності для великих потоків, що робить його незамінним для реалізації сервісів uRLLC та критичних шляхів eMBB. DPDK показав найвищу ефективність обробки дрібних пакетів (до 14.8 млн пак/с) та найкращу програмну гнучкість, що оптимально для площини управління та сигналізації. OVS, особливо в комбінації з DPDK, виявився найкращим рішенням для організації складних віртуальних мереж, забезпечуючи найвищу масштабованість за кількістю підключень (до 1 мільйона), що критично для сценаріїв mMTC.

Застосування технологій прискорення має радикальний вплив на продуктивність. Перехід від базової програмної реалізації до DPDK забезпечує приріст пропускної здатності в 2.1 рази та зниження затримок в 3.9 рази. Впровадження SR-IOV дає ще більш значний ефект: покращення затримок у 7.1 раз. Проте, жодна з технологій не є універсальною: SR-IOV має обмежену масштабованість за кількістю з'єднань (~200 тис.), а DPDK вимагає виділення ексклюзивних ядер CPU. Таким чином, високі показники досягаються лише при цілеспрямованому використанні кожної технології у відповідних їй сценаріях.

Оптимізація життєвого циклу та операційної ефективності Дослідження виявило суттєвий вплик технології віртуалізації на час розгортання та масштабування VNF. Контейнеризовані рішення (Kubernetes) забезпечують значно

швидше розгортання (у 3-4 рази) порівняно з повною віртуалізацією (KVM), що критично для сервісів, що потребують швидкого масштабування. Однак для VNF з високими вимогами до продуктивності та ізоляції KVM залишається необхідним. Оптимальним підходом є гібридна інфраструктура, що поєднує KVM для продуктивних ядерних функцій та Kubernetes для еластичних edge-сервісів і оркестрації.

Розроблений комплексний показник ефективності на основі багатокритеріального аналізу довів свою практичну цінність для прийняття рішень. Методика, що включає нормалізацію різнорідних метрик (пропускна здатність, затримка, використання ресурсів, час розгортання) та призначення ваг, специфічних для кожного сценарію 5G (eMBB, uRLLC, mMTC), дозволила отримати об'єктивне ранжування технологій. Застосування статистичних методів (ANOVA, регресійний аналіз) забезпечило достовірність отриманих результатів та можливість прогнозування поведінки системи.

Аналіз масштабованості показав, що кожна технологія має свої архітектурні межі. Масштабованість за кількістю підключень корелює з ефективністю використання пам'яті: OVS показав найкращий результат, тоді як SR-IOV виявився найбільш ресурсомістким. Для забезпечення еластичності інфраструктури необхідно реалізувати політики динамічного масштабування, що враховують не лише завантаження CPU, але й стан мережевих таблиць, доступну пам'ять та специфіку трафіку кожного сервісу.

На основі отриманих результатів сформовано систему практичних рекомендацій. Для побудови ефективної інфраструктури 5G необхідно прийняти гібридну, політехнологічну модель: використовувати SR-IOV для data-plane шляхів з вимогами до затримки, DPDK для control-plane обробки, а OVS для мережевої віртуалізації та сервісів обробки трафіку. Критично важливим є реалізація централізованого оркестрування (на основі ONAP або аналогічних платформ) для керування життєвим циклом VNF та динамічного перерозподілу ресурсів між різними технологічними пулами.